COMPUTERS AND PRIVACY: A PROPOSAL FOR SELF-REGULATION

EDWARD J. GRENIER, JR.*

In framing the issues in its landmark Computer Inquiry, the Federal Communications Commission cited the critical importance of the preservation of information privacy:

> Privacy, particularly in the area of communications, is a well established policy and objective of the Communications Act. Thus, any threatened or potential invasion of privacy is cause for concern by the Commission and the industry. In the past, the invasion of information privacy was rendered difficult by the scattered and random nature of individual data. Now the fragmentary nature of information is becoming a relic of the past. Data centers and common memory drums housing competitive sales, inventory and credit information and untold amounts of personal information, are becoming common. This personal and proprietary information must remain free from unauthorized invasion or disclosure, whether at the computer, the terminal station, or the interconnecting communication link.[1]

Congress, too, has demonstrated an increasing concern with the possible threats to individual privacy which might result from the establishment, by the federal government or by private industry, of a national data bank.[2] In fact Paul Baran of Rand Corporation, testifying several years ago before a congressional subcommittee, stated that the United States is unconsciously moving toward an integrated, nationwide, automated information system:

> My thesis is this: Today we are already building the bits and pieces of separate automated information systems in both the private and government sectors that so closely follow the pattern to the present integrated communications structure that a de facto version of the system you are now pondering is already into the construction phase. It is in many ways more dangerous than the single data bank now being considered.[3]

Although the threat posed by automated information systems to the privacy of *individuals* is perhaps the most dramatic aspect of the

---

* Member, District of Columbia Bar. B.A. 1954, Manhattan College; LL.B. 1959, Harvard Law School.

1. FCC Notice of Inquiry, Docket, No. 16979, 7 F.C.C.2d 11, 16-17, 8 P & F RADIO REG. 2d 1567, 1572 (Nov. 9, 1966) [hereinafter cited as *Computer Inquiry*].

2. *See generally Hearings on the Computer and Invasion of Privacy Before a Subcomm. of the House Comm. on Gov't Operations*, 89th Cong., 2d Sess. (1966) [hereinafter cited as *Gallagher Hearings*]; Note, *Privacy and Efficient Government: Proposals for a National Data Center*, 82 HARV. L. REV. 400 (1968); *Research Project—Computerization of Government Files, What Impact on the Individual?*, 15 U.C.L.A.L. REV. 1371 (1968).

3. *Gallagher Hearings* 122.

"computer revolution," another very important aspect is the possibility of unauthorized disclosure of *proprietary data*. The "privacy problem" in both of these contexts is most acute where the separate proprietary data of a large number of businesses or sensitive personal information about thousands of individuals is stored or processed in multi-programmed, time-sharing data processing systems and transmitted to and from the processing and storage units over common communications lines. In such systems, there exists at numerous points a high potential for "information leakage," including leakage due to hardware and software failures and wire taps.[4]

In addition to examining both of these aspects of the privacy problem from the point of view of the computer system operator, this article proposes the establishment of a logical legal framework which would serve the public interest by assuring, first, that computer systems which handle sensitive individual or proprietary data will meet certain minimum standards established for the protection of privacy, and, second, that computer system operators will be able to continue to operate in a competitive economy unhindered by either overly restrictive governmental regulation or the fear of private legal liability. The analysis and suggestions herein set forth are relevant to all types of computer systems which store information or use computer programs belonging to persons or entities other than the computer system operator or which collect and store information about private individuals.[5]

The computer industry, which when viewed in its broadest significance extends from manufacturers of main frame hardware to computer service bureaus and computerized information services, should now cooperate with the communications industry to adopt

4. *See* Ware, *Security and Privacy in Computer Systems*, PROCEEDINGS, 1967 SPRING JOINT COMPUTER CONFERENCE 279, 280 figure 1. Effective protection of both individual privacy and proprietary data also demands control over the amount and character of the data input entering the system. *See* Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society*, 67 MICH. L. REV. 1091, 1214-17, 1229-30 (1969) [hereinafter cited as Miller]. Regulation of data input is beyond the scope of this article which is directed solely to controls in the storage and utilization of the data previously collected.

5. An obvious example of the latter is the automated credit bureau. Credit Data Corporation maintains a large scale, on-line computerized credit information system with data centers located in Los Angeles and New York City. Response of Credit Data Corp. to FCC Computer Inquiry, March 5, 1968. *See generally* Miller 1140-54.

and implement, under the auspices of the federal government, a comprehensive system of self-regulation to ensure the privacy and security of data. As a corollary of such a scheme, computer systems complying with the established standards[6] should be freed from certain types of civil legal liability for the unauthorized or accidental divulgence of individual or proprietary information.[7]

THE PRESENT LEGAL SITUATION: A STUDY IN UNCERTAINTY

For the purpose of analyzing the present legal controls pertinent to privacy and the computer, it will be helpful to consider a few illustrative situations:

1. Computer service company A operates a multi-programmed, time-sharing, remote-access data processing system. It services 25 customers scattered over a wide area, each with at least one remote terminal device. Each of A's customers stores at least one proprietary program and a good deal of data in A's system. Companies X and Y are competitors and are both customers of A. Let us suppose that company X has been able to obtain confidential data belonging to Y at X's remote terminal.

2. Assume the same basic set of facts with the exception that A has 500 customers, most of which are very small.

3. Company A runs a computerized information service containing personal data about thousands of individuals, including credit data, medical data, employment data, and educational data. A offers this service to carefully selected classes of subscribers, each of whom promises to use the information for only circumscribed and legitimate purposes.[8] Company A's subscribers are linked to its computer system by remote terminal. Mr. X, a nonsubscriber, manages to tap into company A's system and connect an unauthorized remote terminal, thereby gathering information about a number of individuals. The information so obtained is used in an article which he publishes in a national magazine.

4. Assume the same facts as in example 3, except that a programmer-

6. See notes 54-61 *infra* and accompanying text.

7. This paper does not deal with the problems presented by the *voluntary* disclosure by the system operators of private information about individuals stored in computer systems or questions relating to the accuracy of information about individuals contained in such systems. For discussions of some of the problems involved in the storage of inaccurate information about individuals and the voluntary disclosure of information about individuals, whether accurate or inaccurate, by the custodians of such information, see Karst, *"The Files": Legal Controls Over the Accuracy and Accessibility of Stored Personal Data*, 31 LAW & CONTEMP. PROB. 342 (1966); Sills, *Automated Data Processing and the Issue of Privacy*, 1 SETON HALL L. REV. 7 (1970); Note, *Credit Investigations and the Right to Privacy: Quest for a Remedy*, 57 GEO. L.J. 509 (1969).

8. What constitutes "legitimate" voluntary disclosure of information by the information service company is beyond the scope of this paper. See note 7 *supra*.

employee of company A, without authority, extracts information about some individual from the system and sells such information to Mr. X.

Although the number of possible variations is almost without limit, these four examples are sufficient to illustrate some of the difficulties which computer service companies may face.

From the point of view of the computer service company, the first two examples present issues of contractual or, possibly, tort liability.[9] The customer whose *proprietary* data has been obtained without authority by some third party might well have a claim for breach of contract against the computer service company. However, the results in such a situation can be quite diverse. If the computer service company is dealing with large, sophisticated customers, service contacts are likely to be thorough and well-defined, specifying with detail the degree of privacy and security of data promised by the company and expected by its customer. On the other hand, if the computer service company's customers are small and perhaps less sophisticated, the contract between them may tend to be of the boiler plate variety and may not contain provisions adequate to protect the privacy and security of data. But uncertainty, rather than a complete absence of protection, is more likely to be the case.[10] Unfortunately, the outcome in any specific situation will depend upon the prevailing business practices and governing standards in the state involved.

Examples 3 and 4 squarely raise the issue of the extent to which an *individual's* "right of privacy" will be afforded legal protection.[11] Although most privacy cases involving the disclosure of *individual* information are likely to arise as tort actions, situations could arise in which an individual might have a claim based upon the law of contract. For example, assume that a computer service company enters into a contract with company X to store personal data concerning some one thousand employees of X and to furnish the data to X upon request. Assume further that the contract includes specific provisions for protecting the privacy of the individuals involved. If the computer company breaches the contract by

9. *See generally* Miller 1156-73.

10. *See* Lickson, *Protection of the Privacy of Data Communications by Contract: Another Case Study on the Impact of Computer Technology on the Law*, BUS. LAW, July 1968, at 979-80.

11. Under certain variations of these examples, the contractual rights of the computer service company's customer may also be involved.

allowing information to fall into the hands of a third person who uses it to the injury of the employees, the injured employee might seek recovery against the computer service company as a third party beneficiary of the computer service contract.[12]

In most situations, however, an individual's claim that his privacy had been violated would have to be founded upon the tort of invasion of or interference with privacy. Although of relatively recent judicial recognition,[13] this tort has developed to the point where one noted commentator has been able to discern the existence of four separate torts under the rubric "invasion of privacy":[14] (1) unreasonable intrusion upon the seclusion of another or into his private affairs;[15] (2) appropriation of an individual's name or likeness;[16] (3) unreasonable publicity given to another's private life, or public disclosure of a private fact about an individual;[17] and (4) publicity which places another in a false light in the public eye.[18]

The tort doctrine regarding the protection of privacy, in its present state of development, quite possibly would not provide a basis for a finding of liability against the computer service company in either example 3 or 4, where we have assumed that the computer company took no deliberate action to injure the plaintiff. However, the law of privacy has developed in response to the changing conditions of society, and the advent of the computer age is almost certain to result in a further judicial expansion of the doctrine—perhaps with legislative help.[19] Although four states

12. *See generally* RESTATEMENT OF CONTRACTS §§ 133-47 (1932).

13. The Supreme Court of Georgia is considered to have laid the foundation for recognition of a right to privacy as a fundamental, legally protectible interest in Pavesich v. New England Life Ins. Co., 122 Ga. 190, 50 S.E. 68, 69-70 (1905). Of course, the intellectual foundation for recognition of invasion of privacy as a separate tort had been laid in Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

14. Prosser, *Privacy*, 48 CALIF. L. LAW 383, 389 (1960).

15. *See, e.g.*, Le Crone v. Ohio Bell Tel. Co., 120 Ohio App. 129, 201 N.E.2d 533 (1963) (wiretapping of an individual's telephone).

16. *See, e.g.*, Flake v. Greensboro News Co., 212 N.C. 780, 195 S.E. 55 (1938) (photograph of an actress used in a bread advertisement).

17. *See, e.g.*, Brents v. Morgan, 221 Ky. 765, 299 S.W. 967 (1927) (sign in garage window stating that the plaintiff's account with the garage has been unpaid for a long time).

18. *See, e.g.*, Peay v. Curtis Publishing Co., 78 F. Supp. 305 (D.D.C. 1948) (newspaper article on the alleged practices of Washington cab drivers in cheating the public on fares, making use of the plaintiff's photograph to illustrate the article).

19. For example, Congress is now considering legislation which would regulate the activities of credit bureaus and credit investigating agencies, a field in which the computer has been playing an ever-increasing role. S. 823, 91st Cong., 1st Sess. (1969); H.R. 7874, 91st Cong.,

apparently still reject the right of privacy in its entirety,[20] judicial expansion of the doctrine continues. In *Griswold v. Connecticut*,[21] for example, the Supreme Court seemed to find, in a context quite far removed from the fourth amendment prohibition against unreasonable searches and seizures, a constitutionally protected right of privacy inherent in several amendments.[22]

Of special significance is the recent New York decision in *Nader v. General Motors Corp.*,[23] which extended the *Griswold* rationale prohibiting the violation of a constitutional right to privacy to invasions by a private corporation, not the state. The court implicitly found that state inaction—the refusal by the state court to entertain a lawsuit alleging a violation by the corporation of the plaintiff's constitutional right to privacy—constituted sufficient "state action" to invoke the protection of the fourteenth amendment.[24] If the holding in *Nader* survives, the implications for the computer industry could be far-reaching.[25]

There can be no doubt that the computer service industry, dealing as it does with personal data on hundreds or thousands of individuals, strongly affects the public interest.[26] Indeed, against the background of expanding computer services the need for a further

---

1st Sess. (1969); H.R. 9150, 91st Cong., 1st Sess. (1969); H.R. 9888, 91st Cong., 1st Sess. (1969). The Senate passed S. 823 on Nov. 6, 1969, 115 CONG. REC. 13,905-11 (daily ed. Nov. 6, 1969) and reported it to the House Committee on Banking and Currency on Nov. 12, 1969. Hearings have been held this spring before the House Committee.

20. These states are Nebraska, Rhode Island, Texas, and Wisconsin. RESTATEMENT (SECOND) OF TORTS, ch. 28A, at 100 (Tent. Draft No. 13, 1967).

21. 381 U.S. 479 (1965).

22. *See also* Tchan v. Shott, 382 U.S. 406 (1966), where the Court pointed out that the fifth amendment guarantee against self-incrimination is really in part an extension of an individual's right to privacy and "our respect for the inviolability of the human personality and of the right of each individual 'to a private enclave where he may lead a private life.'" *Id.* at 414 n.12.

23. 57 Misc. 2d 301, 292 N.Y.S.2d 514 (Sup. Ct. 1968), *aff'd*, 298 N.Y.S.2d 137 (App. Div. 1969).

24. *Id.* at 305, 292 N.Y.S.2d at 518.

25. The Appellate Division, in affirming the trial court's refusal to dismiss the case, held that it need not pass upon the constitutional grounds advanced by the trial court. 298 N.Y.S.2d at 141. We shall have to await further litigation to test the implications of *Nader*.

26. *See generally* A. WESTIN, PRIVACY AND FREEDOM (1967); *Gallagher Hearings, supra* note 2; Pipe, *Privacy: Establishing Restrictions on Government Inquiry*, 18 AM. U.L. REV. 516 (1969); Note, *Credit Investigations and the Right to Privacy: Quest for a Remedy*, 57 GEO. L.J. 509 (1969); *Research Project--Computerization of Government Files, What Impact on the Individual?*, 15 U.C L.A.L. REV. 1371, 1374-75 (1968) (foreword by Mr. Justice Douglas).

extension of the doctrine of right of privacy has been vigorously asserted.[27] Thus, one commentator has recently noted that "[t]he concept of privacy held by most courts, considered revolutionary during the Warren-Brandeis era, seems more fitted for the 19th eentury rather than the 20th; a 'new privacy' must be formulated to protect the individual from the technological advances of the computer age."[28] Another commentator recently advanced the thesis that the fifth amendment prohibition against the taking of private property by the government without just compensation, applicable to the states through the fourteenth amendment, should be extended to a similar destruction or diminution of the right of individual privacy.[29] Furthermore, aetions by large public corporations which result in a diminution of an individual's privacy should be regarded as equivalent to state action and therefore subject to the payment of "just compensation."[30] The growing tendency to extend the bounds of privacy protection is thus manifest.[31] If, because of their vast informational storage and ready access capabilities, computers and computer systems become generally regarded as great potential threats to the individual's right of privacy, it would not be surprising to find courts holding computer service companies liable for the

27. Note, *Credit Investigations and the Right to Privacy: Quest for a Remedy*, 57 GEO. L.J. 509 (1969).

28. *Id.* at 532.

29. Comment, *Privacy, Property, Public Use, and Just Compensation*, 41 S. CAL. L. REV. 902, 909 (1968).

30. *Id.* at 913. The author's main point is made in the following statements:

> It can be argued that all large public corporations, such as Time, Inc., whose activity has as great a societal impact as does most governmental action, should be subject to the same constitutional limitations as is the government. Their activity should be labelled "public," rather than "private," in contradistinction to an individual's activity. . . . In short, most corporations are, at least in part, fulfilling interests of the state, and no longer fulfilling the traditional jnstifications of private property. In these instances they ought to be subject to the same constitutional limitations as are imposed upon the state. One of these limitations is that private property cannot be taken for a public use without payment of just compensation. *Id.* at 913-14.

And, as noted, the author would equate the "right of privacy" to "private property" and would require the payment of just compensation for any action which results in a destruction or diminution of an individual's rigbt of privacy.

31. The American Law Institute, in a tentative draft of a portion of a new Restatement of Torts, commented that new forms of the tort of invasion of privacy in addition to the four basic types already generally recognized by the courts may emerge, especially in light of recent decisions by the United States Supreme Court. RESTATEMENT (SECOND) OF TORTS § 652A, comment c (Tent. Draft No. 13, 1967). *See also* Westin, *Science, Privacy, and Freedom: Issues and Proposals for the 1970's, Pt. II: Balancing the Conflicting Demands of Privacy, Disclosure, and Surveillance*, 66 COLUM. L. REV. 1205, 1232 (1966).

unauthorized disclosure of information about an individual.[32] Moreover, the court might go beyond the traditional concept that the defendant must be guilty of an intentional or deliberate wrongdoing in order to be held liable under an invasion of privacy theory and hold computer companies liable for negligently permitting an unauthorized release of information. Indeed, if the information is sensitive enough and the damage from release is devastating enough, a court might be tempted to dispense even with the requirement of negligence and simply hold the computer company *absolutely* liable for the unauthorized release.[33] Whether the computer company's failure is technological[34] or human[35] should make no difference.

The law usually has evolved to keep pace with changing social, political, moral, and economic circumstances. For those who might dismiss as "mere speculations" the above thoughts about the possible evolution of the law of privacy in response to the computer revolution, it would be instructive to consider a statement by Professor Arthur Miller during a recent symposium on the computer and privacy:

> The computer is a many-splendored animal. It is myopic to think of it as little more than a high speed calculator with a gland condition. It's much more than that. Modern information transfer technology in time will prove to be the heart of a new communications network, a communications network that differs from many of the communication networks that we are familiar with, such as telephones, telegraph, radio, television and newspapers, only in technological and media terms. Accordingly, the computer must be dealt with as a communications network.
>
> . . . ,
>
> In short, I am suggesting that we are dealing with a problem of immense importance . . . . [G]iven the large stakes, we should not think simply in terms of the ethical or moral implications of a National Data Center, or any other type of a data center. We must recognize that we are dealing with a new technology, whose applications are just beginning to be perceived and whose capacity to deprive us of our privacy simply cannot be measured in

32. This might prove true whether the companies are service bureaus, information services, or some other type of computer service company.

33. Early manifestations of the theory of strict liability are shown in Huthringer v. Moore, 31 Cal. 2d 489, 190 P.2d 1 (1948); Ball v. Nye, 99 Mass. 582 (1868) (percolation of filthy water); Cahill v. Eastman, 18 Minn. 324 (1872) (underground water tunnel). For an example of statutory extension of this principle, see the relevant portions of the Federal Safety Applicance Act, 45 U.S.C. §§ 1-60 (1964).

34. See, for example, situations 1, 2, and 3, text at 497.

35. See, for example, situation 4, text at 497-98.

terms of existing systems or assumptions about the immutability of the technology.[36]

It is apparent that the legal protection given to the right of privacy is far from static and may, within the reasonably foreseeable future, undergo marked changes. However, except insofar as the changes may be founded upon federal constitutional doctrines, the developing principles may vary markedly from state to state because the basic law involved will be state, not federal, law.[37] For the computer service company, this could mean facing different standards of liability in fifty different jurisdictions for the unauthorized disclosure of information—an unhappy prospect for companies who do a national or regional business.

At present, there is no body of federal law governing privacy which might "preempt" state law as applied to computer systems. After receiving the many detailed and thoughtful comments in its Computer Inquiry and the analysis of the responses prepared by the Stanford Research Institute, as well as the Institute's own recommendations, the FCC has decided that it must await the collection of additional information before deciding whether to exercise its regulatory authority in the area of privacy and security of data during transmission and storage.[38]

---

36. *Symposium: Computers, Data Banks, and Individual Privacy*, 53 MINN. L. REV. 211, 225-27 (1967). The growing concern over protecting privacy in our era of technological explosion is evidenced by the fact that most of the May-June 1969 issue of THINK, the very informative magazine published by IBM, is devoted to a special report on privacy. The articles include Miller, *Psychological Testing: Can We Minimize the Perils?*, THINK, May-June 1969, at 24; Ruggles, *How a Data Bank Might Operate, id.* at 22; Westin, *Life, Liberty, and the Pursuit of Privacy, id.* at 12; Westin, *New Lines Will Protect Your Privacy, id.* at 27. Professor Westin's concluding remarks in his first article are especially illuminating: "American Society now seems ready to face the impact of science on privacy. Failure to do so would be to leave the foundations of our free society in peril." Westin, *Life, Liberty, and the Pursuit of Privacy, id.* at 21. In his second article, Professor Westin points out that many organizers of private data banks, in growing recognition of the privacy problem presented by the computer revolution, are establishing administrative controls to assure the protection of privacy. Westin, *New Laws Will Protect Your Privacy, id.* at 31.

37. *See* Erie R.R. v. Tompkins, 304 U.S. 64 (1938), which laid to rest the notion that there is any generally applicable federal common law to be applied by the federal courts in considering "general" issues in diversity cases. For a more thorough discussion of the *Erie* line of cases, see 1 A. J. MOORE, FEDERAL PRACTICE ¶ 0.318 (2d ed. 1965); Friendly, *In Praise of Erie—And of the New Federal Common Law*, 39 N.Y.U.L. REV. 383 (1964).

38. *Computer Inquiry*, Report and Further Notice of Inquiry, 17 F.C.C.2d 587, 592, 16 P & F RADIO REG. 2d 1505, 1510 (1969); *Computer Inquiry*, Notice of Proposed Rule Making and Tentative Decision, 18 P & F RADIO REG. 2d 1713, 1718 (1970). The regulatory authority of the FCC in this area may, of course, be limited in the absence of additional legislation.

Although it did take a significant step in the privacy area in Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[39] Congress has not acted decisively in this area. In Title III, Congress (1) outlawed the interception and disclosure of wire or oral communications, except as specifically authorized in the statute pursuant to court order;[40] (2) amended section 605 of the Communications Act of 1934[41] to take into account the foregoing addition to the federal criminal code;[42] and (3) established a "National Commission for the Review of Federal and State Laws Relating to Wire Tapping and Electronic Surveillance," which is to study the entire wiretapping and electronic surveillance situation and make a final report within seven years.[43] One interesting feature of this act is that it gives a civil cause of action for damages to "any person whose wire or oral communication is intercepted, disclosed, or used in violation of this chapter . . . ."[44] Although this provision for civil damages in Title III will provide a new, and perhaps potent, remedy to the individual citizen in protecting his privacy, the remedy reaches only one aspect of the privacy problem in data processing, and it certainly does not in any way preempt the various provisions of state law dealing with invasions of privacy. First, the remedy is limited only to persons whose wire or oral *communications*[45] are intercepted, disclosed, or otherwise used in violation of the act. Thus, this remedy on its face does not reach the problem of the unauthorized disclosure of stored information about an individual, which is *not* "communicated" by the individual *himself* to someone else.[46] Secondly, it is not entirely clear whether the act's sanctions

39. 18 U.S.C. §§ 2510-20 (Supp. IV, 1969).

40. *Id.* §§ 2511, 2515-19.

41. 47 U.S.C. § 605 (Supp. IV, 1969).

42. § 803, 82 Stat. 212, 223 (1968) (reprinted in full following 18 U.S.C. § 2510 (Supp. IV, 1969)).

43. § 804, 82 Stat. 212, 223-25 (1968) (reprinted in full following 18 U.S.C. § 2510 (Supp. IV, 1969)).

44. 18 U.S.C. § 2520 (Supp. IV, 1969).

45. As used in the statute, "wire communication" means:

> any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications. *Id.* § 2510(1).

An "oral communication" means: "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation." *Id.* § 2510(2).

46. *See* Miller 1201.

will even reach the problem of interception of data being transmitted to or from a data bank, or the disclosure of such data after interception. The term "intercept," as used in the act, means the "*aural* acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device."[47] Query whether transmitted data is subject to such "aural acquisition," at least in the case of data sent over a special digital communications network using time division multiplexing techniques; query whether courts would reach different conclusions depending upon the technical nature of the communications network over which the data traveled.[48]

A RATIONAL SOLUTION: SELF-REGULATION BY THE COMPUTER INDUSTRY UNDER FEDERAL GOVERNMENTAL AUSPICES

It is estimated that by the late 1970s, the traffic volume over the nation's telephone network will be about equally divided between voice and data transmission,[49] representing a far greater use of the telephone network for data transmission than at present. By 1975 more than 60 percent of the computer hardware used in the United States will be tied into the public communications system, and estimates for 1984 have run as high as 90 percent.[50] Thus, we are on the verge of an explosion in remote access data processing, including a great number of time-sharing, real-time systems. The

47. 18 U.S.C. § 2510(4) (Supp. IV, 1969) (emphasis added). It remains to be seen how the definition will be interpreted. The legislative history of the Act shows clearly that Congress was preoccupied with the interception of voice communications, whether by wiretapping or other electronic devices. *See* S. REP. No. 1097, 90th Cong., 2d Sess. 217-18 (1968). The few cases that have cited Title III of the Act have all been criminal cases or civil antitrust cases closely related to criminal cases and have all dealt with voice communications. *See, e.g.*, Alderman v. United States, 394 U.S. 165, 175 & nn.8-9 (1969); United States v. McCarthy, 292 F. Supp. 937, 943 (S.D.N.Y. 1968); Philadelphia Housing Authority v. American Radiator & Standard Sanitary Corp., 291 F. Supp. 247, 249-50 (E.D. Pa. 1968); United States v. Schipani, 289 F. Supp. 43, 60 (E.D.N.Y. 1968); United States v. American Radiator & Standard Sanitary Corp., 288 F. Supp. 701, 706-07 (W.D. Pa. 1968).

48. For example, the courts might arguably distinguish between interception of data transmitted by the regular analog telephone network and that carried over a special digital network. *See generally* Miller 1206.

49. *See* Chaney, *Data Transmission Basics*, COMMUNICATIONS, Mar. 1969, at 27; *cf.* Irwin, *Computers and Communications: The Economics of Interdependence*, 34 LAW & CONTEMP. PROB. 360, 361 (1969).

50. Note, *Computer Services and the Federal Regulation of Communications*, 116 U. PA. L. REV. 328 (1967).

trends in the law discussed above[51] may well be accelerated by the quickening pace of technological progress.

The choice lies with the computer industry. It can go along and let events unfold in an unstructured, haphazard manner and thereby permit others to fashion for it the basic standards and rules governing the conduct of its business, or it can itself initiate rational means to control its own destiny and at the same time serve the public interest by assuring privacy and security of data, in both transmission and storage. In an industry whose whole thrust is to bring rational order out of the potential chaos unleashed by the information explosion, the choice seems clear: Working from the foundations already laid, the computer industry should pull together, develop, and then enforce standards of construction and operation for computer systems which process data of such a nature that privacy or security are necessitated.

Before detailing the mechanics of this proposal it would be well to point out what is *not* being proposed. The regulation contemplated would not deal with such matters as the rates or prices to be charged by computer service companies, the rate of return they should earn, the terms and conditions of their sales to their customers, or other matters relating to traditional economic or rate regulation.[52] Rather, the industry, under federal governmental auspices, would develop standards to assure that computer systems will incorporate a reasonable degree of privacy protection and will be operated to achieve the desired degree of privacy and security of data necessary in any given circumstance.[53]

Any program of self-regulation should include at least the following features:

1. The program should be specifically authorized and established by federal statute, a prerequisite which would avoid the antitrust problems that inevitably arise where competitors or

51. See notes 13-37 *supra* and accompanying text.

52. The respondents to the FCC's Computer Inquiry, including the Department of Justice, generally agreed that the computer serviee industry should be permitted to develop in the free competitive economy, and not as a regulated utility. *See* L. KRAUSE, *Analysis of Policy Issues in the Responses to the FCC Computer Inquiry*, STANFORD RESEARCH INSTITUTE, REPORT NO. 7379B-2, at 22-26 (1969). The author agrees. For a thorough discussion of the issues involved, see S. MATHISON & P. WALKER, COMPUTERS AND TELECOMMUNICATIONS: ISSUES IN PUBLIC POLICY 16-19 (1970). The FCC, as of this time, agrees. *See Computer Inquiry*, Tentative Decision, 1718-22.

53. These standards should be defined to the greatest extent possible.

potential competitors associate to formulate industry standards.[54] Indeed, the statute should grant a specific antitrust exemption for activities within its scope.

2. Because the program is one of *self*-regulation, some statutory mechanism should be established to permit governmental administrative review of regulatory standards, upon the complaint of interested persons, before they become effective. Such a mechanism would provide customers and potential customers of the computer service industry, as well as private individuals, with an opportunity to express their views on proposed standards.[55]

3. An organization composed of representatives of the computer industry should be established to promulgate and enforce the desired standards. Such an agency should be specifically recognized and granted authoritative powers by federal statute, and its decisions in promulgating standards and in supervising the operations of the computer service industry should be final, though subject to specific types of review by an appropriate government administrative agency[56] and, ultimately, limited judicial review.[57]

4. The industry agency charged with promulgation and enforcement should have the power of periodic inspection to assure

54. For a discussion of the limitation imposed by the federal antitrust laws on schemes of self-regulation within an industry, see Silver v. New York Stock Exchange, 373 U.S. 341 (1963), where the Court cautioned that such schemes will be closely scrutinized because of their potential effect on competition within the industry. *See generally* G. LAMB & S. KITTELLE, TRADE ASSOCIATION LAW AND PRACTICE §§ 11.1-.9 (1956); Baum, *Self-Regulation and Antitrust: Suppression of Deceptive Advertising by the Publishing Media*, 12 SYRACUSE L. REV. 289 (1961); Rockefeller, *Industry Efforts at Self-regulation*, 10 ANTITRUST BULL. 555 (1965); *Developments in the Law—Deceptive Advertising*, 80 HARV. L. REV. 1005, 1159-63 (1967).

55. Such a procedure would afford roughly the same right to comment as is now granted by section 4 of the Administrative Procedure Act, 5 U.S.C. § 553 (Supp. IV, 1969), which provides for the filing of written comments, after appropriate notice, in the case of administrative agency rule making.

56. The author has deliberately refrained at this time from suggesting what government agency should undertake this function. The FCC, with its broad expertise in the communications field, might be the most logical candidate. Perhaps a new agency under the Department of Commerce might best do the job. In any event, the Congress, in selecting or creating the agency to do the job, should take meticulous care to assure that the agency and the whole regulatory scheme will work in tandem with a well defined national communications policy, as well as in furtherance of national policy in the privacy area. *See generally* Miller 1236-39.

57. *Cf.* Silver v. New York Stock Exchange, 373 U.S. 341 (1963), where the Court utilized the federal antitrust laws as a basis for its review of the procedural integrity of a system of industrial self-regulation.

compliance with standards regarding the privacy and security of data.

5. The agency should have specific power at least to conciliate disputes between customers and computer service companies and between individual citizens and computer service companies, arising from, or related to, the standards formulated by the industry agency.[58] Perhaps such conciliation can be made a condition precedent to the bringing of any lawsuit involving the standards or application of the standards.[59]

6. The industry agency should, under guidelines set forth in the federal statute, establish a licensing or certification system for computer systems which will handle information about individual citizens or proprietary data belonging to persons or companies other than the computer system operator. Before any such computer system is permitted to commence operation, it should be required to obtain a license certifying that the industry standards for the protection of privacy and security of data have been met. Such standards should cover not only the technical aspects of the computer system, but also the qualifications of key personnel having access to the system. In connection with the licensing procedure, the applicant should be required to show that it has developed, and will use, appropriate procedures to comply with the standards and to assure that its key employees comply with the industry's code of conduct. As noted above, after initial licensing the industry's agency should have continuing inspection powers to assure that the licensee complies with industry standards. Again, both in connection with initial licensing and any subsequent industry proceeding brought to enforce compliance with standards, there should be review by the concerned governmental agency and, ultimately, limited judicial review. In the event of proposed major alterations in the system, a system licensee should be required to go through a new licensing procedure.

7. The industry agency should have power to promulgate and

58. It may be appropriate to provide for binding arbitration of such disputes instead of merely conciliation. This would be feasible, however, only if the industry agency were a truly independent authority and had such status and reputation for objectivity that nonmembers of the computer service industry would regard it as a fair tribunal.

59. *See generally* W. GELLHORN & C. BYSE, ADMINISTRATIVE LAW 649-51 (4th ed. 1960). For a discussion of the utility of the conciliation process in an analogous context, see 1968 DUKE L.J. 1000 (conciliation procedure in an Equal Employment Opportunity Commission proceeding).

enforce a code of conduct for programmers and other key personnel working with computer systems to which industry standards apply. Sanctions would be imposed upon individuals violating the code of conduct, subject, of course, to administrative review by a government agency and, ultimately, limited judicial review. Such sanctions might include the imposition of fines, with the maximum fixed by statute, suspension from employment, and, in the case of the most flagrant violations, even complete expulsion from the computer service industry.[60]

8. The federal authorizing statute should specifically provide that industry standards will be recognized and given full force and effect in all judicial proceedings, both state and federal. In fact, the statute should provide that, in the absence of an express agreement to the contrary between a computer service company and its customer, the company will not be liable for any loss or destruction of data, or "leakage" of data to unauthorized persons, if the company's computer system has been duly licensed and certified to be in compliance with the industry association's standards, and if in fact the system was in compliance with such standards at the time of the loss, destruction, or unauthorized disclosure. This same exemption from liability should apply in the case of a claim against the computer service company by an individual on account of unauthorized disclosure of data about such individual.[61]

The preceding framework is necessarily a very broad-brush treatment of a highly complex subject. However, if the *idea* of self-regulation is accepted and adopted by the computer industry, the foregoing guidelines can be a point of departure in constructing the

60. Theft of a computer program might be ground for such expulsion. In at least one case, a court has held that computer programs are "property" subject to "theft" under state law, and an employee of a computer company who stole such programs was guilty of felony theft. Hancock v. State, 402 S.W.2d 906 (Tex. Crim. App. 1966).

61. To reiterate, there should be no statutory exemption from liability in the case of voluntary and deliberate acts by the computer service company including companies offering computerized information services. At least as this author now envisions the proposed industry association, it would not deal with criteria for the voluntary release of information to "interested persons," government agencies, or other individuals, groups, or organizations. It may well be that, as the system develops and considerable experience is gained with the arrangement proposed in this article, it will eventually be appropriate for the industry association to promulgate standards governing the voluntary disclosure of information. Of course, to be really effective, especially against the federal government itself, the association should have specific federal statutory authority to promulgate and enforce such standards, and the statute should expressly make them applicable to government agencies.

system. What is needed is a broad consensus within the industry as to the route to be followed, which can then be translated into concrete legislation and a detailed plan of operation.

On the technical side, considerable effort over the past few years has been devoted to developing and improving hardware and software techniques for assuring privacy and security of data during both transmission and storage.[62] In addition, many of the comments filed in the FCC's Computer Inquiry described various techniques used to assure privacy in remote access data processing applications.[63] Thus there is a readily available body of recorded experience and thoughtful comment upon which the standards makers could draw in beginning their complex task.

One aspect of the foregoing proposal for self-regulation must be given special attention. In the case of remote access data processing, the communications links between the remote terminals and the computers must be considered a part of the computer "system" to be licensed or certified if there is to be really effective privacy protection. Yet, in virtually all instances, the communications links will be furnished by common carriers *not related* to the computer service company seeking the license or certification.[64] Thus neither the computer company nor the industry agency proposed above will have control over the degree of privacy protection afforded by a very important link in the computer "system" to be licensed or certified.

The solution to this problem does not rest in making the communications common carriers subject to regulation by the industry agency proposed in this article. Any regulatory scheme which subjects a company to regulation directly by its customers

62. For example, three excellent papers summarizing some of the problems involved in achieving privacy and security of data in multi-programmed computer systems were presented at the 1967 Spring Joint Computer Conference. PROCEEDINGS, SPRING JOINT COMPUTER CONFERENCE 279-90 (1967). The individual articles were Peters, *Security Considerations in a Multi-Programmed Computer System, id.* at 283; Ware, *Security and Privacy in Computer Systems, id.* at 279; Ware, *Security and Privacy: Similarities and Differences, id.* at 287. The terms "security" and "privacy" are used in special senses in those papers, as summarized by Willis Ware in the last-cited paper: "For the purposes of this paper we will use the term 'security' when speaking about computer systems which handle classified defense information which nonetheless must be protected because it is in some respect sensitive." *Id.* The term "security" has been used in a broader sense throughout this article.

63. *See, e.g.*, Response of United States Department of Justice (Mar. 5, 1968), filed in Computer Inquiry, FCC Docket No. 16,979.

64. *See* Irwin, *supra* note 49, at 360-61 (1969); Miller 1099-1103.

must be viewed with at least a healthy skepticism. Thus the communications common carriers should not be subject to regulation by the computer industry agency insofar as these carriers provide communications services in connection with remote access data processing.[65] Moreover, any such attempted regulation of the communications activities of the communications common carriers by the computer industry agency might well conflict with existing regulation by the FCC on the national level and by public service commissions on the state level.

Rather, the solution to the problem would appear to lie in a well-organized system of cooperation between the communications carriers and the computer industry agency, with regulatory assistance from the FCC as required. There should be a continuing formalized liaison between the communications carriers and the computer industry agency, perhaps in the form of one or more representatives of the communications industry working full time in the liaison activity. Such liaison could function effectively in at least two types of situations: (1) when the industry association is formulating privacy protection standards, it should consult closely with the communications industry to assure that tariffed offerings affording the desired degrees of privacy protection in various situations will be available to the computer service industry; (2) if communications problems arise in connection with any particular licensing proceeding under the above proposal, the suggested liaison could help to resolve the problem, possibly through inducing the carrier involved to make a new tariff offering or to amend an existing tariff offering.

Of course, if the liaison activity should fail to resolve any really significant problem, recourse could be had to the FCC or the appropriate state public service commission. To ensure that the FCC will be able to act effectively and expeditiously, the federal statute authorizing the system of industry self-regulation should expressly give the FCC whatever additional power that may be necessary.[66]

---

65. However, if the carriers utilize separate subsidiaries to engage in computer service operations which would be subject to regulation by the industry association if performed by computer companies not related to communications common carriers, such carriers or their computer service subsidiaries should be subject to industry regulation in the privacy area.

66. Even if the FCC might be able to act pursuant to its existing general powers under the Communications Act of 1934, 47 U.S.C. §§ 151-609 (1964), there may be considerable advantage in spelling out the FCC's jurisdiction in this situation and perhaps providing for special streamlined procedures.

If the FCC is to become involved in a significant way in this situation, perhaps it should

There is presently one highly successful example of industry self-regulation under federal governmental supervision. For some thirty years, the National Association of Security Dealers [NASD] has created and enforced a thorough program of self-regulation for the securities industry, including member broker-dealer firms and individual registered representatives. Its principal activities include the administration of examinations to assure the qualfications of employees in the securities industry, the promulgation and enforcement of rules of conduct and fair practice for the securities industry, and the adjustment of grievances betwcen members and between members and the public.[67] One of the most effective tools in NASD's program of self-regulation is its power to examine the books and records of member firms to ensure compliance with NASD rules as well as certain federal regulations. This is equivalent to the inspection program proposed above for the computer industry. In addition, NASD operates a program of voluntary arbitration, both for disputes among its members and for disputes between the public and its members. In the case of disputes of the latter variety, the arbitration panel consists of three members of the public and two representatives from the securities business. In a member versus member contest, the panel consists of from three to five representatives from the securities industry.

Although there are obvious differences between the securities industry and its problems and the computer industry and its

---

be the agency to review actions of the computer industry agency although Congress might wish to consider other alternatives before determining whether to give such jurisdiction to the FCC. See note 56 *supra* and accompanying text.

67. This description of the NASD and its activities is taken from the 1968 NASD President's Report. 1968 NASD ANN. PRESIDENT'S REP. Of interest to the computer industry in formulating its system of self-regulation might be the NASD's statement of purposes:

> (1) To promote . . . the investment . . . and securities business, to standardize its principles and practices, to promote . . . high standards of commercial honor, and to . . . promote among members observanee of Federal and State securities laws;
>
> (2) To provide a medium through which its membership may . . . consult, and cooperate with governmental and other agencies in the solution of problems affecting investors, the public, and [this business] . . . ;
>
> (3) To adopt . . . and enforce rules of fair practice [in the securities business] . . . and in general to promote just and equitable principles of trade for the protection of investors;
>
> (4) To promote self-discipline among members, and to investigatc and adjust grievances between the public and members . . . . CCH NASD MANUAL ¶ 1003.

With some slight change in terminology, many of these statements might be substantially adopted by the computer industry.

problems, NASD constitutes a valid precedent for the type of self-regulatory industry agency proposed herein. By adopting a NASD-type approach, the computer industry can assure the creation of a rational and orderly legal framework for resolving the increasingly pressing problem of privacy in the context of the computer revolution and, at the same time, assure that regulation will be in the hands of persons thoroughly cognizant of the complexities of the situation and the need for protection of individual rights and proprietary interests in data and programs—all to the benefit of the public interest.