Woman C.P.A.

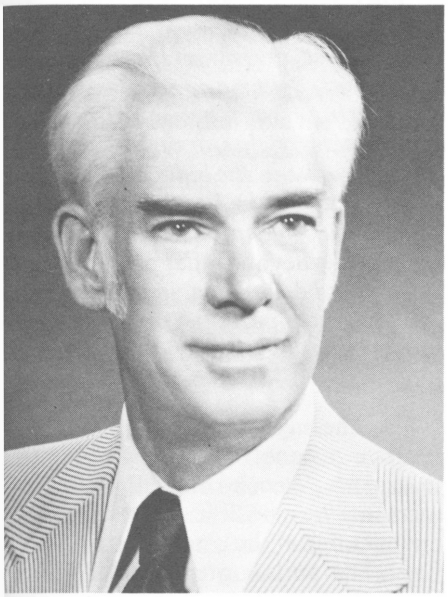
Volume 39 | Issue 2 Article 2

4-1977

Privacy Acts — Implications For Data Processing Managers

Thomas W. Lelievre

Privacy Acts — Implications For Data Processing Managers



Thomas W. Lelievre, CPA, Ph.D

Thomas W. Lelievre, CPA, is Associate Professor of Accounting at the University of Cincinnati. He earned his B.S., M.S., and Ph.D. degrees at the University of Alabama.

He is a member of the AICPA, the Alabama and Ohio Societies of CPAs, and has contributed to various professional journals and publications.

When Susan's 1971 and 1972 personal canceled checks were accidentally destroyed, she needlessly worried about what she would do if she ever needed them. She was unaware that the bank had microfilmed both sides of the checks before they were returned to her. For a nominal fee she could get a copy of any transaction in her bank account. Banks keep such records for a period of five years.

If Susan can request and get copies of her bank transactions, can others also get such information? They surely can. Do others need Susan's approval for access to such highly personal information? They do not! The courts have ruled that the information is part of the records of the bank. They have in effect said that by the use of bank checks we have opened up the details of our private lives to unknown investigators. Since the records are the property of the bank, Susan has no control over their use. The Internal Revenue Service and other governmental agencies have access to this information through the use of administrative subpoena.

An administrative subpoena can be issued by certain governmental agencies without any court action or any notification to the individual. In fact, such subpoenas are used to obtain records on entire groups of people. A major airline was asked for a list of all persons making pilgrimages to one of the gambling centers. The Government was merely fishing for unreported gambling winnings.

Because of its computer a bank in a major city even knew which of its customers paid a hooker the previous night.[1] The bank had installed one of the outdoor machines that allowed customers to withdraw money at any hour of the day or night. The computer records the time that the transaction occurred as well as the amount. The bank, alarmed to discover a strange flurry of withdrawals between midnight and two a.m., feared it was getting ripped off. Investigators discovered that the bank was "convenient to a red-light district," and that customers were stopping for cash en route. On another front, an official in an Eastern city was astounded to be shown a photostat of his check written to a lady of the night for services rendered. The massage parlor was the subject of the investigation - not the city official.

Information stored on numerous magnetic tapes can invade the privacy of every American. All that is needed in many instances is the entering of a social security number into an access terminal. The thought of the unraveling of life histories for indiscriminate purposes has generated vast unease among a wary public.

Many are also rightfully concerned about the validity of some personal information in dozens of different computer files and the improper use of even the valid information. In the midst of potential abuse, what steps have been taken to (1) curtail the collection of this data, (2) insure the validity of the data, and (3) control the use of the stored data? The balance of the article examines some of the governmental and private efforts to meet the brewing problems. The following are discussed: The Privacy Act of 1974, The Commission on Privacy, various state laws, and activities of private agencies such as the AICPA and the Data Processing Management Association.

Past and Pending Legislation

The Privacy Act of 1974 (Public Law 93-579) poses challenges to data processing executives in U.S. Federal agencies. One challenge comes from the meanings of the words "relevance," "integrity," "accuracy" and "security." This same challenge and others will probably confront the remaining public and private sectors in the U.S. in the next few years. The 1974 Act only applied to federal agencies, but legislation is being introduced at both federal and state levels that would extend similar provisions to all public agencies and private concerns. One formidable challenge that will meet private users is that of formulating feasible plans to meet not only the problems already faced by federal agencies, but also, and possibly the greater challenge, problems in the area of cost-benefits.

The Privacy Act provided for a Privacy Protection Commission. The members of this commission were appointed in 1975 and will address the question of whether "privacy" legisla-

Information stored on numerous magnetic tapes can invade the privacy of every American.

tion should be passed to restrict the use and collection of personal information by businesses. This commission expires in June, 1977.

The Department of Commerce is gathering information through a survey designed to determine where possible problems exist and whether the legislation should be extended to private concerns. Its questionnaire seeks to fill the information void with regard to the cost-benefit ratio, the disruption of established business practices, and the possible adverse effects on consumer services. This survey should provide information to Congress for use in further privacy legislation.[2]

The Fair Credit Reporting Act is the principal Act of Congress affecting the private sector's collection and use of personal information. Representatives Koch and Goldwater introduced a bill in the 94th Congress, HR 1984, that would broaden and expand the provisions of the Privacy Act to cover private businesses, state, and local governments. HR 1984 sought to extend to the private sector laws controlling the use of computer data concerning private citizens. It was "a strict, tough" bill patterned after the Privacy Act of 1974. It covered all manual and automated data systems which "describe, locate, or index anything about an individual, regardless of whether the system is private or public."

After the introduction of the Koch-Goldwater bill, DPMA (Data Processing Management Association) sponsored a symposium on the Impact of Privacy Legislation in Washington in May of 1975. Feedback indicated that implementing the act in the form of its introduction would be "overburdensome, not cost effective, and almost too obtrusive to the point of becoming detrimental not only to business but to the consumer himself."[3] The bill was not passed by the 94th Congress, but the sponsors hope for enactment of a similar measure in the present session of Congress and believe that the essential points will eventually become law. However, it appears that Congress will not act until after the privacy commission makes its report in 1977.

Other proposed federal legislation (drafted by a House Judiciary subcommittee) includes a new privacy protection bill covering police departments and similar data banks. One section of the proposed bill is devoted to "secondary use." It limits what can be done by organizations and individuals with dossier data they obtained from law enforcement agencies. Previous bills attempted to control secondary use only by limiting access to data bank files.

Various bills are appearing in state legislatures. *Data Management* (April, 1976) reports the introduction of such legislation in California and Minnesota. S.B. No. 99 was passed in the regular session of the 111th General Assembly of the State of Ohio and became law on July 21, 1976. This bill "regulates the use of personal information by state and local governments and requires governmental and private computer systems to give public notice of its existence, to protect the privacy of individuals from excessive record keeping by government." More than 125 bills to protect privacy are pending in various legislative bodies.[4] Since the thrust of this paper concerns problems arising from Privacy Acts, only the provisions of the federal act will be discussed. This decision arises from the belief that future acts will probably contain similar provisions, but would extend to all governmental agencies and private sector concerns.

Quotes From the Privacy Act of 1974[5]

1. *The opportunities for an individual to secure employment, insurance, and credit, and his right to due process and other legal protections are endangered by the misuse of certain information systems (preamble).*
2. *Federal agencies (will)... be subject to civil suit for any damages which occur as a result of willful or intentional action which violates any individual's rights under this Act (preamble).*
3. *Each agency... shall... establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.*
4. *Whenever any agency . . . fails to maintain any record concerning an individual with such accuracy, relevance, timeliness, and completeness as is necessary to insure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual... the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction.*

The message of these quotes must become a concern of data processing managers. Agencies of the U.S. Government are responsible for the integrity and security of the personal data in their files. The author predicts that similar laws will be drafted and enacted that will extend privacy legislation to state and local government units and to all private organizations. Thus, the challenge of meeting the integrity and security requirements is here for all data managers.

Integrity and Accuracy of Data

Writing in the April, 1976 *EDP Analyzer*, Richard G. Canning distinguished between the integrity and the accuracy of data. He used accuracy to mean "conforming exactly to the truth: and integrity to mean "the data system does not inject error into the system." Thus, the two words together would mean that the data is "undistorted by error." However, if erroneous data is entered into the system, the system cannot correct this, but acts with integrity if it does not inject more error into the data. Thus, the burden is on the organization to see that erroneous personal data never enters the system. To insure the integrity of the data the injection of error must be inhibited during the initial recording, transmission, processing and storage, as well as during the recovery process.

Errors can never be completely eliminated; each organization must find

its own error tolerance level. The big question is whether the tolerance level that is acceptable for operations is good enough to meet the demands of privacy for personal data. Errors made in financial data may be easily corrected; seldom are the reputations of individuals personally affected by such errors. Granted, persons may make financial investments of erroneous data and be monetarily hurt, but such losses can be compensated by damage awards. Erroneous information or the misuse of personal data puts an organization in an entirely different game; one that is played by entirely different rules. Even the rule makers are different: in the financial information area the Securities and Exchange Commission (SEC) is the principal regulator; the proposed national legislation would probably be regulated by a Privacy Commission; the Fair Credit Reporting Act by the Federal Trade Commission (FTC), and the proposed legislation covering the "secondary use" of information in data banks by the Justice Department.

Improving Data Integrity

The first step in improving data integrity might be to develop definitions for personal data. There are not any nationally accepted definitions as yet. Such definitions must be developed before national standards can be developed or applied. Such definitions should include the characteristics of accuracy, relevance, completeness, timeliness, and verifiability. Once definitions are developed, a next step might be to review and possibly redesign the forms and procedures for collecting data. If some piece of data is not relevant, its collection should be dropped. Outdated information should be deleted. For the protection of the organization, information that cannot be independently verified should be deleted. The entire process of data entry should be reviewed to improve the detection and correction of erroneous items, and to prevent their reentry into the system. The internal control system used for such data should be reviewed on a regular basis.

The FTC served notice that it would question data collection procedures when it filed a formal complaint in February, 1974, against the Retail Credit Company.[6] The complaint accused Retail Credit of such violations as setting daily work loads so high that investigators had to falsify information to meet quotas and required investigators to file a percentage of derogatory reports to impress its customers. Also questioned was the problem of disclosing the sources of information that entered the files. Disclosure of the sources of information is not presently required. Retail Credit insisted that the required disclosure of information sources would "seriously" impair the company's investigations. Retail Credit's problem areas were in preemployment and insurance investigations. Unlike the credit reports, where much of the information is available in public records, preemployment and insurance investigations involve contacting an individual's neighbors and business associates to ask questions about the subject's life-style, financial and marital situation, and drinking habits. Critics insist that people should have the right to see these files to correct what Ralph Nader called "backyard gossip."

The question of the accuracy and integrity of computer programs must be considered, as well as the data itself. In a multi-programming job stream one program can change another program, and another program can change the data. Thus, a number of things should be reviewed concerning the way that personal data is stored and handled. One suggestion is that "dedicated equipment" might be used for particularly sensitive applications, both for security and integrity. The feasibility of such an approach might be questioned since it might play havoc with integrated systems.

The problems of the real quality and relevance of data are separate from that of systems errors. The quality of data is measured by its accuracy, relevance, and precision. Data might be accurate but not relevant to the decision, or not relevant for multiple purpose use. Precision is an indicator of the repeatability of the measurements used in the determination of accuracy. It is the consistency (or lack of it) of one method of measurement repeated numerous times. "Precisions is affected by what is under the control of the decision maker - his operations of measurement transcribing, values of attributes, and the stability of his processes."[7] Thus, the precision of information may differ between investigators due to different attitudes and procedures. This is usually referred to as interviewer bias. This lack of precision between investigators has no doubt added to the problems of credit reporting agencies. Canning restates the accuracy provision in the following way:[8]

the challenge of meeting the integrity and security requirements is here for all data managers

Collect information from a variety of independent sources, including the data subject, when the information may result in adverse determinations about the individual's rights, benefits, and privileges. Moreover, these sources should be chosen on the basis of most likely disagreement. Then indicate the estimates of accuracy and precision for each data item recorded about the individual.

Security of Data

Data security is the safety of data from accidental and/or intentional but unauthorized disclosure, modification, destruction, or theft. Most computer administrators have installed controls to safeguard their installations and data files, but are those steps adequate under the demands of privacy legislation?

Illegal use of computer credit data was the subject of a December 29, 1976 consent order of the FTC against collection practices of a debt-collection subsidiary of Diners Club, Inc. The subsidiary, National Account Systems, Inc. was accused of illegally tapping computer banks of credit information and using the data to harass debtors. The company was accused of abusing telephone code numbers to effectively steal information about debtors from computer data banks operated not for bill collection but for insurance companies and credit institutions. NAS agencies, using unauthorized code numbers, told the computer companies that they had subscribed to the credit information.

In the order the government served notice to the bill collectors of America that it no longer will tolerate strong-arm tactics or unauthorized use of computer information about debtors. Some view

precision of information may differ between investigators due to different attitudes and procedures

the order as a landmark case because of its significance in the area of privacy of consumers. It is the first time that the FTC has issued an order involving violation of the Fair Credit Reporting Act, which attempts to govern the use of "the big computer in the sky." It is also the first time it has issued an order against anyone for obtaining information under false pretenses. Under its statutory authority the FTC can apply judgments against a single respondent to those throughout a particular industry: thus all debt collection services must heed the standards contained in the consent order.

Decisions regarding internal security practices are completely up to management. Thus, management must decide *how much* security is required. How much security is needed to guard against the loss or misuse of data, for the day-to-day operations of the system, and against the unusual case that cannot be anticipated nor identified in advance? Should HR 1984 have been enacted as drafted, any person who violated that Act would have been liable for the actual damages sustained by the data subject, punitive damages where appropriate, and court costs. Furthermore, violations might be interpreted to include "insufficient" data integrity and security. How far should an organization go toward enhancing its data integrity and security practices? Canning suggests six possible alternative approaches to bring the threat of lawsuits within accpetable bounds:

1. **Make no changes.** With this approach, management decides that the present data integrity and security practices are adequate, and that no enhancements probably will be needed. This approach involves the least additional cost for data integrity and security and probably has the least credibility in the event that law suits are brought under the privacy act.
2. **"Prudent man" principle.** Under this approach, the organization makes a threat analysis and risk analysis concerning the personal data in its files. Once the threats and risks have been identified, the decision would be made on what to do and what not to do on the basis of what the "prudent man" who is concerned about protecting his own property would do. To what extent the courts would side with the "prudent man" decisions is debatable.
3. **Decision algorithms.** This approach is similar to the "prudent man" approach except that formalized, quantitative methods are developed for making the decisions on what to do and what not to do. These methods would probably use the cost/benefit approach. A short-coming of this approach is that the decision of which method to use would be subjective, dependent upon the opinions of a small number of people. How much weight these opinions would carry in court is also a matter of conjecture.
4. **Accreditation of installation.** This approach requires that some independent agency, governmental or private, develop standards for data integrity and security practices. No such standards presently exist. The agency should probably represent the federal government and the industry-wide computer field. A data norm might be developed that would consist of general principles, standards that support and define these principles, and guidelines that explain and give practical examples of applying the standards. The agency would also develop and apply formal accreditation methods. With accreditation and standards which are professionally developed and nationally applied, the courts might still rule in favor of the plaintiffs, but it would appear less likely than in the case of the "prudent man" principle.
5. **Certification of the installation.** As with accreditation, the certification of computer centers would involve the development of standards. Authorized individuals or organizations would inspect data centers and certify (or fail to certify) that the centers met the standards. The model might be that of CPAs who perform audits and give an opinion on the financial statements. Certification differs from accreditation in that the certifying individual or organization would have a legal responsibility. Of course there is no guarantee that standards of data integrity and security would not be challenged in court, but it appears likely that the courts would usually side in favor of the standards.
6. **Licensing of the installation.** Control by licensing would provide that personal data could neither be collected nor maintained unless the organization obtained a license from the government. A license would be granted only if the organization agreed to meet standards of integrity and security. Obviously, the license could also be withdrawn. Such licensing is not being considered in the U.S., but Sweden requires that all maintainers of mechanized files of personal information must be licensed.

The Costs of Privacy

Data processing officials no longer wonder whether their work will be affected by privacy legislation, but how to deal with the controls that are certain to be imposed. Since more than 125 bills to protect privacy are pending, one must conclude that after the question, "What will my company have to do to comply?", comes another question, "How much will it cost?" There will no doubt be high conversion costs in changing present systems to systems that would comply with legislation and legally protect organizations.

A major contribution to the privacy conversion cost figures will arise from the requirements dealing with the physical security of data. A second major cost will be associated with training the operators and users of the system in privacy-oriented procedures. It is sometimes surprising to discover how many individuals have access to a system and therefore must be given the

special training. Many of the users of a systems may not be employees of the organization operating the system. This raises important questions about who should give the training, who should pay for the training, and who should be responsible for enforcing the training requirements at each facility.

The computer programming needed to develop some of the capabilities to satisfy the legislation will also be significant. Goldstein estimates that in some cases it accounts for as much as one-third of the total conversion costs. Once the conversion is completed, the additional costs will not cease, expecially if the major impact of a change involves people. The critical costs are executive and clerical time, assuming that the present computer installation has the capability of handling the additional work load.

The 1974 Act and most of the proposed legislation includes requirements that all personal data be maintained in an adequate state of accuracy and timeliness. A fraction of the data in systems will become obsolete each year and must be deleted. Goldstein estimates this to be approximately 10 percent, which would require clerical costs that might run from 26 to 45 percent of the total annual privacy cost. Complaints about an individual's record would probably be handled by an administrator in a hearing process. Such a formal process could prove costly in terms of administrative work load, assuming that the volume of complaints is at an annual rate of .2 percent of the number of records in the system.

In summary, it appears that it will be quite expensive to meet the privacy requirements of proposed legislation. Some organizations may discontinue their installations, while others may pass part of their increased costs on to others. Some cost reductions might be realized from the further automation of procedures.

Actions of the Accounting Profession

The accounting profession is aware of the potential impact of pending legislation on all compilers and users of information. In the Spring of 1976 the Institute appointed a Special Committee of Privacy Legislation. Essentially, the committee is charged with monitoring and analyzing proposed privacy legislation as to how it may affect Institute members and their clients' data systems. At the annual AICPA meeting in October, 1976, the chairman of the special committee reported that the current status of the accountant's role in privacy legislation is in flux, but that the committee was working on a response to the Federal Privacy Protection Commission with which the accountants can live. At this writing the contents of that response have not been publicized.

Congressman Goldwater appeared as the keynote speaker before the Annual AICPA Conference on Computers and Information Systems held in Philadelphia in May, 1976. He told of the continuous invasion of privacy by governmental and private organizations and how the bill grew out of the increasing concern of citizens over the invasion of what may be considered their inalienable rights. Those rights given by the fourth amendment to the Constitution are:

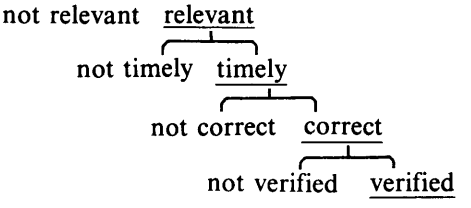
> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated,*

Businesses as well as CPA firms will be involved in implementing any legislation that passes, through improved data security and controlled accessibility. One principal area of concern is personnel administration — particularly accessibility to personal information and the uses to which that data can be applied. An example of the improper use of such personal information was given by a guest psychiatrist on a morning TV program in early 1976 concerning the bad experience of one of his patients. This patient came to him complaining of a very bad nervous condition that she attributed to the unkind words and actions of fellow employees at her place of employment. The psychiatrist diagnosed the condition as being a type of schizophrenia although the patient was not told the specific diagnosis. Her first medical insurance claim was filed with the insurance company which forwarded the data to her place of employment, where it was entered in the personnel data bank. The first morning of her return to work she was greeted by three different co-workers with expressions of sympathy as to her illness with reference to the diagnosis of schizophrenia of which she was unaware. She became greatly upset, immediately resigned her position, and the psychiatreist stated the public divulgence of such personal information as to her illness together with the conditions under which it was broadcast had a very serious effect.

what will my company have to do to comply?...how much will it cost?...

Conclusion

Only the tip of the iceberg has been considered in this paper. In spite of such a limited consideration, there appears to be little doubt that privacy protection will become a part of all data systems that contain personal information. The time is at hand to discuss how the integrity and security of these systems are to be protected. Organizational planners must include plans for meeting these challenges and for considering the resulting costs. Kenneth T. Orr suggests that, "good privacy and security are simply good management" and that privacy will be cheaper if a firm only keeps data that follows this hierarchy:[9]



FOOTNOTES

[1]William Bierman, "Who's Afraid of the Big Bad Computer?", *The Enquirer Magazine,* September 12, 1976, p.41.

[2]Francis M. Gregory, Jr. and Wright H. Andrews, "The Privacy Debate," *Data Management,* August 1975, p. 32.

[3]"Privacy Update, An Interview With Congressman Barry Goldwater, Jr.," *Data Management,* February 1976, p. 31.

[4]Robert C. Goldstein, "The Costs of Privacy," *Datamation,* October 1975, p. 64.

[5]Richard G. Canning, "Integrity and Security of Personal Data," *EDP Analyzer,* April 1976, p. 1.

[6]"Critics Zero in on Retail Credit," *Business Week,* 6 April 1974, p. 60.

[7]Canning, p. 8.

[8]Canning, p. 9.

[9]Kenneth T. Orr, "Data Security and Privacy," *Infosystems,* February 1976, p. 34.