Transborder data flow: legal persons in privacy protection legislation

by SUSAN H. NYCUM and SUSAN COURTNEY-SAUNDERS
Chickering & Gregory
San Francisco, California

SYNOPSIS
In view of current proposals to establish treaties and privacy protection guidelines on transborder data flows, it has become necessary that the United States adopt a position on whether "legal person" be included in such treaties and guidelines. The following discussion attempts to evaluate the various arguments and concludes that the United States, based upon its own definition of privacy, regulation of "legal persons," and economic and foreign policy, must maintain that "legal person" be excluded from privacy guidelines.

DISCUSSION
A. Introduction

Inclusion of "legal persons" in regulation of privacy with regard to transborder data flow encompasses sociological, political, economic and philosophical issues. Review of the issue of protection of individual privacy is not enough. While certain nations seek control of transborder data flow through access to its use, process and content, other nations desire to foster an atmosphere of free enterprise and competition by permitting business to remain relatively free of governmental or private intrusion.

Including "legal persons," or natural persons and business entities, in privacy protection may inhibit the free flow of data and free exercise of competition. If business entities are included in privacy protection, any business files would be open to inspection and correction by any individual or other business mentioned in those files. As a result, customers, potential customers, competitors, and suppliers would have the opportunity to inspect the files of the particular business. Such disclosure may be so harmful to business that it cannot function effectively in that country.1

On the other hand, privacy rights may actually be further protected if business entities are entitled to inspect data concerning them. This may be the case when an individual's privacy interest is so identified with a business entity's interests that the individual's privacy can be more fully protected through disclosure of business records to him. Also, certain countries have political, economic or social reasons for including legal persons in their privacy legislation, not the least of which is to exclude competition presented by the foreign data industry.

The United States must consider its own policies on privacy regulation and international commerce and other countries' concerns in order to protect its own individual, corporate and national interests and to harmonize them with interests of other nations.

This paper will first outline current definitions of "legal persons," existing privacy protection legislation covering transborder data flow (hereinafter TDF), and current proposals for treaties and guidelines on privacy regulations and TDF.

Next, arguments for and against inclusion of "legal persons" in privacy protection will be presented.

Finally, the considerations the United States must address on this issue, and the recommendations it might make, will be discussed.

B. Existing and proposed privacy protection in TDF regulation

1. Definition of "legal persons"

In order to examine the inclusion of "legal persons" in TDF privacy protection, a single definition must be agreed upon.

Under the Internal Revenue Code, a "person" is an individual, trust, estate, partnership, association, company or corporation.2 Under the New Bankruptcy Act, "person" includes an individual, partnership or corporation.3 Although the Freedom of Information Act defines "person" as including "an individual, partnership, corporation, association, or public or private organization other than an agency," the Privacy Act limits its protection to "individuals" or "a citizen of the United States or an alien lawfully admitted for permanent residence."5 The Right to Financial Privacy Act provides access to financial records by any "individual or a partnership of five or fewer individuals."6

Authorities on TDF regulation have stated that a "legal
person' does not have to be a legal entity, but can be any group of persons or any business enterprise. If "legal persons" are to be included in the group protected by TDF privacy regulation, then the definition of "persons," based on the above authorities, would probably be natural persons, groups of persons, and any business entity including a sole proprietorship, corporation or partnership. For purposes of this report, "legal persons" will signify all the above entities except natural persons in order to distinguish regulation solely of natural persons from regulation of both natural and business persons.

2. Current privacy protection legislation


The Swedish Data Bank Statute is the earliest regulation of TDF and privacy. It requires all domestic and foreign data banks containing personal information to be licensed by the Data Protection Board before they begin operation in or with Sweden. A registration list containing the information stored or transmitted on persons must be given to the Board. The protection extends only to private persons, who may request from the Board any information in the list concerning them. Section 1, 16. Thus, Sweden does not include legal persons in its privacy legislation.

b. West German republic: federal data protection act, 1977

This Act provides for a private data administrator at each business storing data on individuals. This administrator decides what categories of privileged information are to be stored and what processing to use. Section 29. Also the Act provides for disclosure by the government of data held on individuals. Sections 7-21. The German Act covers only physical persons. Section 2(1).


This bill provides only individuals, and not legal persons, with the right to obtain, examine and correct records concerning them held by or for the Canadian Government. Part IV, Section 49, 52.

d. France: act no. 78-17 of 6 January 1978 concerning computerized indexes and the protection of the liberties

The French Act requires that any entity desiring to establish a data bank must obtain an authorization from the National Commission for Data Processing and the Liberties. Chapter III, Art. 14. Also, any data bank must be open for inspection and correction only to individuals. Chapter I, Art. 4; Chapter V.

e. Norway: personal data registers act of 1978

This Act requires that data banks obtain permission from the King in order to establish personal data registers. Chapter 4, Section 9. The "personal information" covered by the legislation includes "information . . . traceable to identifiable individuals, associations or foundations." Chapter I, Section 1. Thus, those Norwegian "persons" protected include both individuals and business entities.

f. Denmark: bill on private registers 1978

The Danish Bill requires data banks to register with the Register Board prior to communication to any third party in Denmark. Chapter 3, section 14. Legal persons are included in this privacy protection because "[a]ny systematic collection and registration of information on the financial conditions of persons, associations or undertakings" may take place only in accordance with the act. Chapter 1, Section 1. The act provides that any "person" may inspect any information about themselves held by any registered entity. Chapter 2, Section 7.

g. Austria: act on data protection, 1978

The Austrian Act requires private data banks to register with and obtain a license from the Federal Minister, including data transmitted abroad unless the receiving country has a data protection law similar to the Austrian law. Chapter II, Section 9; Chapter V, Section 25. The act includes legal persons by defining "personal data" as "information, including personal identification marks, relating to a natural person or a juristic person or a 'personal company' in the sense of commercial law." Chapter I, Section 2.

h. Luxembourg: act regulating personal data use in data processing, March 1979

This Bill requires any data bank using a Luxembourg data processing means and containing personal data to obtain authorization by a competent minister and registration with a general directory. Chapter 2, Section 4.5. The Bill defines persons as "any natural person . . . [e]ach corporate body under Luxembourg law, from time of constitution, (or) any other corporate body registered in a Luxembourg Public Administration or a Social Security establishment register." Chapter 1, Art 2. All "persons" have the right to inspect and correct data contained in any data bank registered with the National Directory. Chapter 5, Art. 19,20.
Legal Persons in Privacy Protection Legislation


The Freedom of Information Act (FOIA) provides the mechanism for any “person,” including an individual, partnership, corporation, association, or public or private organization, to be provided, upon request, with any non-exempt record held by a government agency about any “person,” except information that would, if disclosed, violate national security, trade secrets or other confidential business information, attorney-client privilege, or, balancing the interest served by the exemption (e.g., privacy) against the public interest served by disclosure, information on individuals may be withheld. 5 U.S.C. §552(b)(1-7).

The Privacy Act permits any “individual” or citizen of the United States or an alien lawfully admitted for permanent residence to inspect records only when held by any government agency. It also prohibits disclosure by a government agency of any record of an individual without the written consent of the individual if the record constitutes a clearly unwarranted invasion of personal privacy, such as medical files. The FOIA’s balancing to determine the exemption from disclosure for individual data is not present in the Privacy Act, which provides for a clearer restriction on disclosure. 5 U.S.C. §§552a(b), §552(b)(6).

Neither act provides for disclosure of information by private entities to either natural or legal persons. Bills are pending in the Congress which would extend such coverage to the private sector.

Privacy protection extends to providing the right to examine records held by private entities, however, under the Right to Financial Privacy Act, 12 U.S.C. §401, et seq., which permits individuals or partnerships of five or less to inspect information on them held by any public or private financial institution, and the Fair Credit Reporting Act, 15 U.S.C. §1681, et seq., which permits individual consumers to inspect credit reports held by a consumer reporting agency.

3. Current and proposed TDF international treaties and guidelines

a. The council of Europe

The 20-member Council of Europe (COE) expects to ratify its treaty on data protection, including privacy protection, by 1980. The U.S. will have the opportunity to be a signatory along with Japan, Canada and Australia. Whether the U.S. signs the treaty or not, it will be affected. The purpose of the COE treaty is to establish common rules among nations on the rights of the individual when an automated record on the individual is gathered, processed, and transmitted across borders. The treaty must consider and reconcile the issues involved: protection of the rights of the individual, preservation of the free flow of information, and recognition of the supremacy of national law and variations in legal systems. It will represent only minimum rules and each nation can expand the scope of protection.

The current treaty draft does not cover data on legal persons. However, the drafters are trying to provide a mechanism for cooperation between those nations including legal persons and those excluding them. Frits Hondius, Division head of COE in Strasbourg, France, indicates that the “legal persons” issue has not yet been resolved by the COE: “Where a legal person should be able to claim the same protection as a natural data subject is a controversial question that needs careful study.”

b. The OECD

The U.S. is participating in the drafting of guidelines for the cooperation on TDF issues by the Organization for Economic Cooperation and Development (OECD).

The OECD has omitted from its third draft a section providing that its guidelines would not restrict any nation from applying privacy protection beyond natural persons “to groups of persons, associations, corporations or any other bodies whether or not such bodies possess legal personality.” Its current intention is therefore to exclude “legal persons” from privacy protection, replacing that clause with:

“3. These Guidelines should not be interpreted as preventing the application of different protective measures to different categories of personal data depending upon their nature and the context in which they are collected, stored, used or disclosed. Furthermore, nothing in these Guidelines should be interpreted as preventing countries from applying them only to the automatic processing of personal data.”

c. OECD vs. COE: the need for uniformity

While the COE concentrates on the issue of protecting individual rights, the OECD is looking at the total economic, cultural, and social impact of regulating all kinds of data flow. Both the COE, in treaty form, and OECD, in guideline form, recognize the importance of uniform data flow regulation among countries. However, a treaty affords a much higher level of protection to data subjects than guidelines. Because European countries already have data protection laws in force, the guidelines stage may have already passed. According to Hondius, “Common guidelines are a useful first step for legal cooperation between states,” but since laws are already in force in many countries, “a legally binding treaty is necessary . . . in order to solve conflicts of jurisdiction.”

To date, privacy protection legislation differs in scope of coverage, data subjects and enforcement. For example, the U.S. and Canadian Privacy Acts only compel public entities to disclose information held on individuals, while all the other countries with such regulations also compel disclosure by private entities. While Norway, Denmark, Austria and
Luxembourg include legal persons in their privacy legislation, the other countries with privacy legislation do not. While some countries enforce their legislation through private agents at each data bank, others require state licensing or an authorization. This diversity leads to more costly data processing for foreign data companies because they are required to constantly investigate and comply with varied legislation. This will inhibit multinational data transport. In addition, diverse legislation could also require transmission only to those countries with reciprocal protection laws, as in the Luxembourg Act. The only way to alleviate these problems is to establish ground rules for emerging international data networks through guidelines or treaties with the goal of setting up "an international regime of well-defined, preventive rules . . . for the feeding, operation, and use of international data networks to guarantee maximum safety of the systems not only from a physical point of view but also from an information quality point of view."19

C. Arguments on for and against including "legal persons" in privacy protection

1. For inclusion

The primary reason for privacy protection is to assure the individual an opportunity to limit, inspect and correct personal information recorded in any data bank. Thus, Swedish legislation contains special controls over information on an individual's political or religious views, whether they have received social welfare or have been treated for alcoholism.20 The concern is that privacy may be violated by accumulation of information and dissemination where the individual does not want it to go.21 The proponents of inclusion argue that this individual privacy right can only be preserved if privacy legislation is extended to legal persons.

Luxembourg's new privacy protection legislation states that inclusion is a matter of avoiding discrimination which would result from treating individual and corporate financial information differently:

"It is within the context of this new individual right that must be placed the issue of the citizens protection area. The opinion of the Commission is that a new discrimination must not be created by refusing above listed rights to corporate bodies. This would mean institutionalization of a gap. It is customary for financial establishments to keep information on their customers credit rating. In the event that an inaccurate information would be stored in a banking establishment, the commercial firm which is the bank's customer must, as the case may be, have the right to request correction of data whose inaccuracy has been verified. Could this right to correction be refused to certain categories of persons? The Commission does not think so. This is why it approved the government draft which is widening the scope of the law to natural persons and corporate bodies."22

The French first considered inclusion of legal persons because it would provide small firms with the opportunity to find out what big firms knew about them: "Originally, both business and government were favorable to this inclusion . . . the French employer's association . . . believed it would allow firms to find out what data the government and other state institutions held on them."23

Another reason for including legal persons which specifically addresses individual privacy is that in some cases the interests of a natural person can be so intertwined with the interest of a legal person that the natural person's rights can only be fully protected if legal persons are also covered.24 For example, information concerning a small business' financial situation may reveal the personal financial situation of its president. Also, there is a sense of unfairness in the idea that an individual craftsperson is protected but if he incorporates, he is not.25 Beyond simply preserving privacy, the data protection legislation tends to control the political and economic side effects of data transport.26 Nations concerned with preserving national sovereignty, developing their own data processing industry, and controlling cultural influences have and will consider privacy protection legislation, with the inclusion of legal persons, as a means of protecting these interests.

Sovereignty and economic concerns focus on who controls data flow. At present, data flow has a lopsided nature. Multinational computer services and the telecommunication industry are primarily located in one place, the United States. Countries interested in developing their own domestic computer services face stiff foreign competition because importing information and services is less expensive than developing local industry. Also, national sovereignty may be threatened when foreign control of data exists because nations fear being cut off from such data.27 Finally, this technological and economic dependence by smaller countries creates cultural conflicts over the influx of foreign media data, in some cases causing rejection of technology or disruption of social order.28

Developing nations are also concerned that the multinationals centered in the U.S. create a serious unemployment problem because data processing takes jobs from the minimally skilled workers in their countries. Any contrary argument that the new industry creates jobs must be careful to distinguish the new, skilled labor jobs created by multinationals providing countries with processed data from the unskilled jobs lost through their replacement by mechanization.29

Another economic concern of developing nations is the competition the foreign data industry has on their state-owned Postal, Telephone and Telegraph (PTT) administrations. The issue is that foreign private networks divert their revenues.30 All the above economic and political concerns lead nations to consider legislation to prevent these problems. Including legal persons in privacy protection is one way to alleviate some of the problems by regulating the foreign data processing industry to the point of either removing it altogether from their country or severely limiting its influence.

2. Against inclusion

Focusing on the foremost reason for privacy legislation, individual privacy, the proponents of excluding "legal per-
sons" from privacy protection argue that privacy by definition cannot be an attribute of a "legal person" because the nature of individual privacy interests differs from those of business entities. Since privacy legislation concerns itself primarily with the accumulation of personal social data, such as religious and political affiliations, the reasons for protection cannot extend to legal persons, whose data is financial or proprietary. Also, legal persons' "privacy interest" is already fully protected by confidentiality and trade secret legislation.31

A special fear associated with privacy protection which includes "legal persons" is that the skillful use of access rights can distort competition.32 If the right of access is extended to legal persons, it would mean that competitors could find out what was on file and divulge proprietary information.33

To the countries which are against inclusion, more control of "legal persons" would not encourage individual freedom from intrusion, but would, on the contrary, be the first step in stifling personal privacy by increasing state control of information transmitted in or out of a nation by the private sector,34 and would ultimately signify government control of commerce and trade,35 resulting in lower productivity and slower development of the data processing industry.36

Another concern is the cost of privacy legislation that includes legal persons. Because European countries have and will, even in the face of the minimum COE treaty proposal, enact inconsistent privacy protection laws, multinational TDF companies must spend revenues to determine if their existing and planned record-keeping procedures are lawful.37

Also, it is argued that smaller countries have the most to gain from unfettered movement of information across their borders. Since none of the smaller countries is technologically self-sufficient, those that restrict free flow will impede their own economic growth.38

Finally, inclusion of legal persons may create "Data Havens" by excluding companies from countries with TDF regulations. Those countries with no laws restricting the use of data would acquire the data banks causing a loss of control of domestic information and revenues in regulated countries.39

D. U.S. position on "legal persons": economic and foreign policy compel exclusion

1. U.S. privacy right and business entities

Because the right to privacy developed in the United States excludes corporations, the U.S. would be supporting a policy contrary to its own privacy if it supported inclusion of "legal persons." The legal right to privacy was most clearly articulated in Roe v. Wade, 410 U.S. 113 (1972):

"... the Court has recognized that a right to personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution. ... These decisions make it clear that only personal rights that can be deemed 'fundamental' or 'implicit in the concept of ordered liberty' ... (such as) activities relating to marriage, ... procuring ... contraception, ... family relationships, ... and child rearing and education." 410 U.S. at 152-153.

In United States v. Morton Salt Co., 338 U.S. 632, 652, 70 S.Ct. 357, 94 L.Ed. 401 (1950), the Supreme Court ruled that corporations have no privacy right equal to individuals and therefore could not resist an FTC subpoena on invasion of privacy grounds:

"[C]orporations can claim no equality with individuals in the enjoyment of a right to privacy. [Citations omitted]. They are endowed with public attributes. They have a collective impact upon society from which they derive the privilege of acting as artificial entities."

The Privacy Act prohibits disclosure of personal records by government agencies on "individuals," U.S. citizens or aliens with permanent residence, except to that individual, and does not provide business entities with the same protection. 5 U.S.C. §552a. Business entities are covered by the FOIA, but not under the "privacy" umbrella. The FOIA requires any government agency to disclose to anyone information held on natural and legal persons except where disclosure would reveal trade secrets or confidential business information. 5 U.S.C. §552(b)(4). This exception to disclosure has been interpreted to cover not only trade secrets, but "any commercial or financial information ... if its disclosure is likely ... to cause substantial harm to the competitive position of the person from whom the information was obtained." National Parks & Conservation Assn. v. Morton, 498 F.2d 765, 770 (U.S.C.A., D.C. 1974).

Further, trade secrets and commercial or financial information which is privileged or confidential may not be disclosed by any employee of the U.S. in trade negotiations under the Federal Advisory Committee Act, 19 U.S.C. 2155(g)(1)(A), and disclosure of such information by any government employee subjects him to a fine or imprisonment. 18 U.S.C. §1905.

If the U.S. were to recommend inclusion of legal persons in privacy protection, information would be available which is now exempt from disclosure because of the harm disclosure would do to competition. This would contradict the federal position as stated in the FOIA and Federal Advisory Committee Act that business' trade secrets and confidential information must not be disclosed, and would expand privacy protection expressly limited to individuals in the Privacy Act to include legal persons.

The U.S. has limited the scope of privacy protection legislation, by considering the use and nature of the information and how that use and nature corresponds with the U.S. right of privacy. Specific concerns, such as governmental intrusion, which is prevented by the Privacy Act and the FOIA, and financial records, which are available to individuals and small companies which would be most harmed by a secret blacklist, are addressed. But a broad, sweeping control of information in order to protect the right of privacy does not exist. If the U.S. is to be consistent with its domestic privacy protection in its international recommendations, it must use
this sectional approach, examining the use and nature of the information before recommending control over it.

Part of this recommendation, however, must be that legal persons be excluded from privacy regulation to avoid permitting inspection of confidential business information harmful to competition.

2. U.S. foreign policy: free enterprise, private participation and cooperation

The U.S. position found in legislation on foreign economic policy further demonstrates that its support of inclusion of legal persons in privacy legislation would be inappropriate. Congressional policy on international development requires respect for individual civil and economic freedom. 22 U.S.C. §2151(a). Foreign policy goals must include:

"(3) the encouragement of development processes in which individual, civil and economic rights are respected and enhanced; and

(4) the integration of the developing countries into an open and equitable internal economic system." 22 U.S.C. §2151(a)(3)(4).

Also, free enterprise is explicitly a part of the U.S. foreign policy:

"(a) The Congress of the United States recognizes the vital role of free enterprise in achieving rising levels of production and standards of living essential to economic progress and development. Accordingly, it is declared to be the policy of the United States to encourage the efforts of other countries to increase the flow of international trade, to foster private initiative and competition . . . to discourage monopolistic practices, to improve the technical efficiency of their industry, agriculture, and commerce, and to strengthen free labor unions; and to encourage the contribution of United States enterprise toward economic strength of less developed friendly countries." 22 U.S.C. §2351(a). (Emphasis added.)

By agreeing to include legal persons in privacy legislation the U.S. would violate its articulated foreign policy goals because it would thereby support the suppression of free flow of trade and private enterprises.

E. U.S. recommendation: omit legal persons from privacy protection

Clearly, the U.S. interest is in preserving the free flow of data. The U.S. must also encourage a unified TDF policy which considers all the issues, including the economics, sovereignty and independence, of other countries. In view of U.S. domestic privacy legislation, which provides privacy protection only for data categories posing great risks to individual privacy, and its foreign policy, which encourages free flow of data and free enterprise, the U.S. should urge that legal persons be excluded from privacy protection.

FOOTNOTES

2. Internal Revenue Code: IRC §7701(a)(1).
5. 5 U.S.C. §552a(2).
7. Pantages, Europe Moves Toward Controlled Data Flow, Datamation, Nov. 1, 1978, at 82, col. 1; Second Draft Guidelines Governing the Protection of Privacy in Relation to Transborder Data Flow of Personal Data, by OECD, Feb., 1979, at 8, permitting guidelines to include:

"Groups of persons, associations, corporations or any other bodies whether or not such bodies possess legal personality." (Omitted in 3rd draft but quoted here to demonstrate a common definition of "legal persons.")

10. Pantages, supra at 80, col. 1.
11. 3.1 Council of Europe Resolution (74) 29 On the Protection of Privacy of Individuals Vis-a-Vis Electronic Data Banks in the Public Sector, which states:

"... the adoption of common principles in this field can contribute towards a solution of these problems in the member states and can help to prevent the creation of unjustified divergencies between the laws of the member states."

13. Id., at 82, col. 1; Council of Europe Resolution, supra:

"For the purposes of this resolution, personal information means information relating to individuals (physical persons) . . . ." Id. at 1.

17. Pantages, supra, at 81, col. 1.
18. Luxembourg Bill Regulating Personal Data Use in Data Processing, March, 1979 Chapter 2, sec. 1, art. 5(2); P. Hirsh, Europe's Privacy Laws—Fear of Inconsistency, Datamation, Feb., 1979, at 85, col. 3.
19. Hirsh, supra, at 85, col. 3, quoting Hans Peter Gassman, on the architects of the OECD draft guidelines.
21. Canadian Department of Communications and Department of Justice, Privacy & Computers, Task Force Report, Ottawa, 1972 at 1, 14.
"Information is power and economic information is economic power. Information has an economic value, and the ability to store and process certain types of data may well give one country political and technological advantage over other countries. This, in turn, may lead to a loss of national sovereignty through supranational data flows." Donaghue and Longsworth, supra, at 23.

30. Novotny, supra, at 5.
31. R. Turn, supra, quoting Joinet at 5.
32. Id.
34. Hirsh, supra, at 85, col. 3; Novotny, supra, at 2.
35. Donaghue and Longsworth, supra, at 24.
36. Datamation, Canada's Economic Concerns, Nov. 1, 1978, at 67, col. 3. Duties on foreign computer equipment bought by Canadian companies make domestic development of data processing expertise too expensive, so the Canadian computer industry is against government protection intended to limit U.S. competition.
37. Hirsh, supra, at 85, col. 3.
38. Id., at 87, col. 2.
Simulation

Simulation is one of the oldest application areas for computers. Traditional users of simulation include the aerospace, military/defense, process control, industrial control, and energy industries. Newer users of simulation include corporate management, private and governmental planning agencies, and small businessmen. The NCC sessions describe advances in traditional areas such as process control as well as new applications such as the modeling of computer software, decision support systems for business management, futures planning, and small business decisionmaking. A particularly significant growth area is the use of simulation to explore the effects of decisions and alternative futures. This area is represented by sessions on decision support systems, cross-impact models, and small business applications.

The simulation of complex engineering systems has long been a major application of computers. Tremendous activity has occurred in flight simulation, the analysis of aerospace and military systems, the modeling of chemical and physical processes, and the design of power plants, reactors, and other large, complex systems. This activity is continuing and is being affected by new computing techniques, new computer languages, and new software packages. The session on "Advances in Process Control" investigates the effects of new hardware, software, and methodology on the process control industry. The paper by Gordon and Robinson on "Using preliminary Ada in a process control application" describes the use of the U.S. Department of Defense standard language ADA in process control. The paper by Sagues on "Computer aided heat penetration tests for the food canning industry" describes the use of small minicomputers in test automation.

Meanwhile, computers themselves have created new modeling problems. The modeling of computer performance is a well established application area. The modeling of computer software, a newer area of interest, is being explored in a panel session entitled "Software Models: History, Current Status, and Future Directions." Topics of concern will include reliability and quality assurance models, model validation, and the needs of the software community.

Among the more intriguing applications of simulation is its use in predicting the future course of events or at least exploring the effects of alternative decisions or alternative time histories. This use becomes particularly important in a time of rapid change and great uncertainty. Decision support systems provide top management with the ability to explore the effects of decisions with a reasonable expenditure of time and money. User-oriented planning languages allow rapid formulation of problems in a comprehensible form. The panel session on "Decision Support Systems" describes the effective use of decision support systems, the advantages of modern planning languages, and the importance of decision support systems in data processing organizations.

The session entitled "Simulation—A Planning Tool" describes the use of cross-impact models in long-range planning. Cross-impact models are based on the effects of events on each other—that is, whether the occurrence of a particular event increases or decreases the probability of the occurrence of other events and by how much. The most fully developed cross-impact model is the INTERAX world model developed by the University of Southern California's Center for Futures Research. This session will include an overview of cross-impact models and a description of the INTERAX model, emphasizing its goals, methods, and uses. The paper by Rosenthal entitled "A cross-impact simulation forecast of the data processing industry" describes the use of the INTERAX model in simulating the evolution of the emerging data processing industry.

New and less expensive computers allow the use of simulation in areas where it was formerly too expensive. Small business is a primary example, since minicomputers and microcomputers now provide low-cost computing power in an area with the same basic problems as larger businesses. Typical applications of simulation will be explored in a session entitled "Simulation in Small Business." Topics to be explored include strategic systems modeling, investment analysis, business forecasting, and the presentation and analysis of simulation results.

Lance A. Leventhal
Area Director