SHARE

SHARE SESSION REPORT

61	M311	Trans Border Data Flow		65
SHARE NO.	SESSION NO.	SESSION TITLE		ATTENDANCE
Security			O. Lee Hurtt III	SSI
PROJECT			SESSION CHAIRMAN	INST. CODE

Southern Company Service, Inc., 64 Perimeter Center E., Atlanta GA 30346 (404) 399-3344

SESSION CHAIRMAN'S COMPANY, ADDRESS, AND PHONE NUMBER

The Security Project is pleased to present Mr. Harry B. DeMaio as the Speaker for this session. He is the Director of Data Security Programs for the IBM Corporation. He is especially well qualified to speak upon this subject because of his knowledge and experience.

Harry DeMaio joined IBM in 1956. He has held a series of management positions in marketing, systems engineering and development. As Director of Data Security Programs, he has worldwide responsibility for ensuring that all IBM divisions have appropriate plans and product offerings to support customer requirements for systems security, auditability and systems management.

He is also responsible for directing IBM representation worldwide to individual national governments, intergovernmental agencies, the media, industry and professional organizations on the issues of computer systems security, auditability and systems management as well as the broader social issues of privacy protection and international information regulation.

He is a member of the State Department Advisory Committee on transborder data flow, as well as the International Chamber of Commerce and CBEMA committees on transborder data flow.

This subject is of vital importance to all organizations conducting business in the international market. As Mr. DeMaio notes, the flow of information is the essential element of this topic. This, he develops his theme on the International Information Environment.

0/F/rcg/1

INTERNATIONAL INFORMATION ENVIRONMENT

Harry B. DeMaio
Director of Data Security Programs
IBM Corporation
Old Orchard Road
Armonk, NY 10504
SEC
M311

ABSTRACT

Discussion of the International Information environment in this briefing paper is divided into its component issues. Each issue is treated in overview fashion with national and international illustrations provided, and several additional policy recommendations which do not readily fit into the individual issue discussion are provided.

This paper is by no means a comprehensive catalog of issues or experiences. It does try to highlight the principal areas of debate. Recent history indicates that the relative importance of current issues will change and new issues will emerge with some frequency.

The increasing acceptance of the phrase "International Information Flow" over "Transborder Data Flow" reflects the broader nature of the issues and constituencies involved. "Information" covers a much wider spectrum of usage and policy involvement than the word "data" which is usually interpreted as "technical or business data." Since "information" can take on many more forms, it therefore serves a much wider user base and involves many more providers and sources. Similarly "transborder" focused attention exclusively on the movement of information across national boundaries. However, many of the components of this issue involve the ability of international companies and other organizations to use locally generated information and facilities within the boundaries of a given country.

The component issues of International Information Flow have been categorized a number of different ways in the past and specific situations often fit more than one category. However, it has now become commonly accepted in national and international policy discussions that IIF has the following characteristics:

(I) Protection of Human Rights - primarily the privacy issue
(II) National Security
(III) Economics
(IV) Political & Cultural Integrity

Involved in each of these categories are a number of interest groups.

(a) Information suppliers
(b) Information equipment and services suppliers
(c) Telecommunications providers
(d) Users of all or some of the above
(e) National and international regulatory and legislative bodies
(f) National and international standards, and similar cooperative bodies

Obviously any given organization, institution or government may at any given time fit more than one of these interest areas. This may in turn create conflicting objectives and perspectives for that government or institution.

The Privacy Issue - In Europe, the term "transborder data flow" originally emerged from the desire of countries having privacy legislation to protect sensitive personal data moving outside their boundaries to the same extent that it was protected inside. This "data protection" emphasis resulted from a belief that computers and telecommunications, with their ability to collect, manipulate and transmit high volumes of information rapidly and inexpensively, represented a unique threat to personal privacy. This approach resulted in an emphasis on protecting sensitive information in electronic form but said relatively little about that same information in so-called manual form. It also placed the government in the position of regulator, registrar (or licensor) and inspector of sensitive files. The European approach differs from U.S. policy perceptions in at least four areas:

(a) U.S. reliance on voluntary self-regulation by information owners and users to the greatest degree possible;
(b) U.S. concern for protecting sensitive information in any form rather than computerized information only;
(c) Individualized U.S. legislation (federal and state which is tailored toward the specific characteristics of individual sectors where control is deemed necessary; e.g., medical, banking or credit, government, employer-employee) as opposed to the blanket coverage of the European model;
(d) U.S. reliance on the courts to provide redress for actual abuses rather than an anticipatory licensing structure.

In view of these differences, the establishment of a worldwide agreement has been difficult. There are two international instruments at the moment: the Council of Europe Treaty, which has been initialed but not yet ratified by member states, and the OECD Privacy Guidelines. While both documents are aimed at creating a common denominator of harmonization, the OECD Privacy Guidelines are more compatible with the U.S. approach since they are more cognizant of the value of voluntary compliance. The private sector in the U.S. has responded favorably to a request from the Department of Commerce for endorsement of the guidelines.

There is another element in European privacy legislation which needs some explanation: the concept of protecting the legal person. In several countries, the legal person (corporations, partnerships, organizations, etc.) is specifically covered by additional provisions of the legislation. This means that with a few exemptions all files and applications dealing with sensitive information (e.g., credit ratings, performance, quality) about vendors, customers and competitors must also be licensed or registered and are open to inquiry by the data subject. Austria thus far has gone the furthest to comprehensively implement the legal person program. Certain European service bureau offerings were delayed in Austria while determination was made of what protection and registration responsibilities rest with the data owner and user (the customer) and with the caretaker (the service provider).

There has been some comment made about the possibility of the legal person being used as grounds for government fishing expeditions into corporate business data. Thus far, we know of no experience to directly bear out this concern, but the overall experience base is very small indeed. It is our expectation that most future legislation will contain legal person provisions, at least in Europe.

Is privacy an exhausted issue? No. First, there remains a substantial number of countries, European (e.g., U.K., Italy) and non-European (e.g., Japan and most of South America) which are just considering or have not yet begun to consider privacy legislation. Secondly, most privacy laws leave a great deal of discretion to the licensing bodies and, therefore, the privacy policy of most governments is still only partially described or understood. Third, several countries are working to revise their legislation (Sweden and Germany). Finally, there are additional proposals for stronger international instruments

coming from within the European Parliament and the Council of Europe which, while not imminent, still cannot be ignored.

Proponents of the existing legislative and regulatory structures for data protection in Europe argue that the burden of compliance on corporations and other institutions has not been insurmountable and relatively few files have been restricted or refused licensing. What is not clear is how much additional protection has resulted from these activities. Unfortunately, that measurement is probably impossible to develop. However, there have been some cutbacks in the administrative support for the Data Commissions in several countries indicating that the governmental cost has exceeded expectation or may not be sustainable in the face of current economic conditions.

In short, while U.S. privacy laws and policies will continue to require clarification and explanation in world forums, we do not believe there is a requirement for fundamental change.

National Security - It should be obvious as we progress through this analysis that the lines of demarcation between categories are very dim and ill-defined. National security and economics are good examples of this definitional problem. While there is little argument that sovereign governments have the right and obligation to defend their citizens, the use of national security in IIF discussions has gone well beyond the traditional concepts of national defense.

In the context of U.S. national security, DoD restrictions on technology transfer, both in hard and soft form, have had occasional impacts on the strength of U.S. arguments in support of unrestricted flows in other countries. While the principle of strategic technology control is itself valid, great care needs to be taken that the principle is being implemented consistently and only where clearly necessary.

Two countries have led the move to a broadened use of the national security platform--Sweden and Brazil.

Sweden, in the SARK report and subsequent commentaries, treats its entire information infrastructure as having "strategic significance" and also evaluates its current status as vulnerable. The prospect of a nationwide general strike led Sweden to consider that a similar effect might be produced by a relatively small number of information workers who through strike or sabotage could stop the railways, airlines, telephone systems, press, or government. A similar result could probably be produced by a hostile foreign government. If information services were supplied from systems or suppliers outside of the country's borders, the vulnerability to deliberate or accidental loss was assumed to be that much greater. This led to several proposals: (1) that distributed systems by spreading the vulnerability are preferable to centralized ones. This is by no means accepted by the security community. A strong case can be made that distribution creates control problems that in many cases outweigh the advantages; (2) that a licensing function be created for certain classes of system application based on the system's "robustness." This licensing would be an additional function of a national privacy protection authority. The technical, administrative, economic, standards and governmental implications of such a system are profound indeed, but thus far have been explored very little. In 1981, the OECD sponsored a conference to examine some of these characteristics. Fortunately, the atmosphere at the conference was primarily one of information professionals seeking to improve the state of the protection art. There is still a great deal to be done in the area of systems protection. The computer and telecommunications industries in general have been responsive to requirements. It is our belief that broad-based standardization and government licensing in this area are not conducive to optimum security. This is an area in which responsibility is shared by a broad spectrum of users and suppliers. Much of the solution is non-technical--dealing with personnel, organization structure and end-user responsibility. Government encouragement and sponsorship of research and education in this area are important. Licensing and restrictive control on a broad basis is impractical and potentially destructive.

Brazil, the other primary example of a national security view, leads ultimately into the category of economics. Brazil has taken the approach that its information policy should be driven toward minimizing external dependency for all forms of information support. This policy has economic motivation; e.g., balance of payments and growth of indigenous industry, but it also has the security motivation that no external agency, nation or company will be capable of impacting Brazil through deprivation of technology, equipment and parts, software or information itself. Therefore, new equipment and software purchases from outside Brazil require government approval. Approval is based primarily on lack of a Brazilian capability to supply a similar function. The same ground rules apply to data base suppliers, computing services and telecommunications services. To further control these services, a governmental agency has been established to screen and license incoming data offerings.

It is difficult (and perhaps not very relevant) to assess how much of this is true security vs. economics. The difference may become important if the OECD, IBI, UNESCO or other international organizations embark on a significant security program and choose the Brazilian model for its agenda. The prospect of economic barriers being erected in the name of national security will no doubt be undesirable for Brazil's trading partners.

Obviously, one of the primary sources of protection against being made captive to a single national source is the development of the unrestricted world markets the U.S. has been advocating.

Economics - In the past two years, this has become one of the major items on the IIF agenda. As indicated previously, privacy and national security overlap with some of the items contained here. It has not been unusual to find organizations, committees, working groups, etc, with a mandate for one aspect of IIF to be deeply embroiled in another.

The USTR has prepared a comprehensive listing of barriers to trade in information services with country references. It is not our intention to reproduce that work here.

A comprehensive list of barrier mechanisms would include:

(1) Restrictive Legislation
(2) Taxation and Customs
(3) Standards
(4) Telecommunications Policies and Tariffs
(5) Work Rules
(6) Procurement Policies
(7) Subsidies or Direct Government Development

This section will give illustrations of certain classes of barrier or policy activity and their impact.

One thing should become clear during this discussion. Most of the mechanisms required to carry out a program of IIF economic restrictions already exist in most countries and would require little more than administrative decrees or regulatory interpretation to become effective. Major new legislation is typically not required.

Restrictive Legislation - The Brazilian example already given is a case where direct legislation was used to create barriers. Brazil probably has the most clearly enunciated informatics economic policy. While other countries like France and Canada have made major public statements in this regard, Brazil has implemented a national program. As noted above, in those countries outside of North America where PTT monopoly of telecommunications exists, where major commercial information users such as airlines and railroads are nationalized, where the central bank's influence is often stronger, where the government - labor union relationships are closer and where radio - TV are government-owned or controlled, - government influence is already sufficient to make major new legislation unnecessary to create a controlled environment.

In various degrees, the Brazilian economic restrictions affect all the major interest groups. Data base suppliers are restricted in how and what they can market from outside Brazil. Data processing equipment and service suppliers are similarly controlled. As in most countries, telecommunications services are a government monopoly. Users must also seek permission for procurement of certain classes of hardware. Control of software procurement is currently under discussion. Both SEI, the approval body, as well as the standards and rate-setting bodies, are part of the Brazilian policy mechanism. There have been no other major examples of such direct and comprehensive legislative programs although the Canadian Bank Act and FIRA are cited in this regard and there is potential for legislative activities in Mexico.

Taxation and Customs - The major driving issue here is the emerging consideration of information as a commodity. The underlying theory is that information can be classified and valued as an asset, bought, sold and traded. Therefore, it would follow that information responds to commodity classification and treatment, especially in a customs and value-added tax sense. Less developed countries through UNESCO and the IBI have taken this commodity idea to a different end and have expressed the North/South problem in terms of "information rich - information poor" countries. Parity in information has been cited as an international goal.

The obvious fact is that information is in a unique class of its own. While certain types of information are subject to priced exchange, the value is usually based on the service, the medium or some underlying product or good rather than on the actual information itself. Further, information is not consumed in any commodity sense. If anything, it expands with consumption. The vast majority of information exchange is of the non-commercial variety and even within the commercial sector, is primarily made up of intra-enterprise, administrative or transactional exchanges in support of movement of goods or services.

As services, especially services with high information content, become more dominant elements in the GNP's of all countries, developed and developing, this issue will no doubt continue to surface, if for no other reason than a search for a taxation mechanism. It is for this reason alone that much work must be done in the services trade area to develop agreements which include information transfer. However, it must be clearly defined where trade in services and information transfer do and do not coincide. In spite of a considerable overlap, there are issues unique to each.

To ensure this overlap is properly handled, user involvement is key in all of these considerations. Let us illustrate with the following example. If a country or region seeks to protect its national airlines from foreign competitors, one of the many techniques available is to deny or restrict foreign carriers access to a national reservation system. The information specialist may see this as a classic case of information control. It may, however, be part of a broader program which includes other forms of discrimination like denial of gate space, landing rights, personnel restrictions or higher landing fees. Similarly, attempts to control or restrict other information intensive industries such as banking, insurance, shipping or international credit will certainly involve but not be limited to information exchange restrictions. The banker or airline executive will no doubt have a different view of how and where these issues should be pursued than the information specialists. These users may be understandably reluctant to watch an issue which they regard as specific to their industry move to a more generalized form. Such choices should certainly rest with the primary user.

How can the principle of free flow be clarified to reflect the diversity of meaning of the concept? First, we should begin to abandon the word "free" and substitute the word "unrestricted." This will help to end the argument about the inherent contradiction of charging a fee for services which is a form of restriction in itself. Obviously, most uses of the word "free" in the U.S. position papers really refers to lack of restriction, not lack of pricing. Europeans and some third world countries have unfortunately misinterpreted this not only in the context of trans-border flows but also on the question of technology transfer. Consistent use of the more precise wording will hopefully reduce these semantic arguments and permit more useful discussions.

Secondly, the concept of an unrestricted market must be introduced into the discussions, which will place in clearer relief the ideas of both tariff and non-tariff trade barriers and their impacts on the structure and dynamics of that market.

Standards - The development of discriminatory standards for the underlying purpose of restricting the ability of manufacturers to market competitive products or preclude users from having the flexibility of choice between differing products or services can be viewed as a non-tariff trade barrier. This is a misuse of the standards development process and all affected groups must guard against such discriminatory practices.

There are major areas of standards development with potential for such discrimination. Subjects like Open Systems Interconnection (OSI), Local Area Networking (LAN) and Integrated Services Digital Networks (ISDN) are only a few of those impacted by the development of standards for the interconnection of systems, equipment and services. Of particular concern are the current efforts of CCITT on the definition of ISDN, which is especially important to users, manufacturers and carriers. These efforts will establish technical standards and policy/services directions for the future use of telecommunications services and for those services and products using telecommunications services.

The proper application of the standards process is to yield standards which provide compatibility, interchange and interconnection for the benefit of all interested groups without imposing discriminatory restrictions.

Such efforts must not restrict the flexibility to permit the development and beneficial use of new technologies when these standards are implemented. The CCITT, the ISO, the IEC and individual national standards bodies are the primary organizations involved in the standards development process.

Telecommunications Policies and Tariffs - This is a major arena for IIF concern. The rules under which individual countries or regions will authorize the classes of service to be supplied and the rates to be charged are fundamental to the IIF issue.

One of the basic issues is the future use in foreign countries of flat-rate private line service by information suppliers and information service suppliers including special purpose networks like SWIFT - the inter-bank network.

There are several illustrations which outline foreign PTT efforts to preserve their current revenue sources and to maintain control over future service markets. The first is the Japanese KDD's reluctance to supply service to two U.S. based data servicers, Tymshare and Control Data. The conditions under which service was eventually granted included restrictions to access specific computer systems at a specific computer center without rights of further interconnection within the U.S. While there has been some removal of these restrictions as a result of appeals to the Japanese Minister of Posts and Telecommunications (multiple systems may now be accessed), there are still operating restrictions in place which curtail these service offerings.

In December 1978, the West German Bundespost announced regulations which sharply curtailed the use which could be made of international leased channel circuits by foreign data servicers wishing to supply remote access service in Germany. Essentially, they require that all leased lines entering Germany terminate in a single terminal device that is not connected to any other German network or to a computer that performs "true" data processing (not simply switching) of the data. This means data servicers must have a data processing facility in Germany in order to effectively do business there. These regulations have been the subject of a great deal of question, negotiation and slipping of effective dates of new services. It is not clear (in itself a problem to those planning information processing in Germany) what the outcome will be. The State Department among others has been engaged in a series of negotiations and queries on this area.

The Brazilian strategy outlined above, a service issue in Hong Kong similar to the KDD issue, discriminatory tariffs by Euronet to U.S. data base suppliers, are other recent examples.

A second telecommunications policy issue concerns the regulations affecting use of privately owned equipment for connection to the public telecommunications network as well as the interface procedures. Such regulations can severely limit the type, make or design of such equipment and the type of communication and data services that can be provided to users.

A third issue is restrictions by national governments and regions on competitors of their PTT's offering of enhanced telecommunications services. This type of restriction stifles the offering of new services and products to the public.

Understanding of this area is essential for an understanding of the IIF issue but as should be apparent, IIF and telecommunications policies intersect but do not totally overlap.

Work Rules - This is an area which has not occupied center stage but has some impact. As a brief example, the Worker Councils of several Scandinavian countries and in Germany have won cases upholding their refusal to work weekends or off-shift. The impact on a seven day, 24 hour global network is obvious. Similarly, some of the ergonomic areas cited above are also the result of work rules. Many countries have operator-to-machine ratios which were developed to deal with sweat-shop environments. In at least one instance (Mexico) these rules were suggested for data processing installations. While certainly not of the same magnitude as some of the other issues noted, the potential disruptive influence of work rules can still be quite significant.

Procurement Policies - There are many examples of discriminatory government and nationalized industry procurement policies in this area. The Japanese government is only one significant example in telecommunications and computing equipment, information services and software. Obviously, as government influence extends through the PTT monopoly structure, nationalized users and other institutions like universities and research organizations, the impact can

be substantial. The Office of the U.S. Trade Representative has documented many examples of procurement situations.

Subsidies or Direct Government Development - France, Brazil and Japan are three major examples of countries embarked on direct subsidy or government development programs. The Japanese sponsored an R&D consortium for VLSI chip development which directly propelled them into worldwide chip contention. France has embarked on a series of "Plans Calcul" to subsidize computer, service and telecommunications development and has in the past two years engaged in substantial government sponsored marketing activites in Africa, South America and the U.S. A substantial advertising and display campaign at U.S. computer conferences by the French took place in 1981. The Mitterand government has given indications of continued support for these activities.

Regional Economic Activities - In addition to individual countries, regional activities must also be taken into account. Such organizations as the European Commission and European Parliament have been actively engaged in studying the impact of "micro-electronics." The OECD has a major work plan within its ICCP Committee devoted to economic issues. The IBI has created work parties on this and other areas and its SPIN Conference will no doubt include economic discussions. Probably less well known but of more direct impact is the IBI's consultative activities in South America and Africa on individual telecommunications projects. UNESCO has primarily dealt with the human rights side of these issues but UNCTAD, UNCSTD and the UN Center for Transnational Corporations have become active in these issues with studies and work programs.

Political and Cultural Integrity - This concern manifests itself in several ways. As international telecommunications makes it increasingly possible for businesses and institutions to operate inside a country's borders while maintaining most of their assets and resources outside the borders, the question of erosion of national government authority surfaces. Other phenomena have also triggered this concern: so called "stateless" currencies transferred over worldwide networks; satellite footprints crossing national borders and making foreign television signals available to anyone with an antenna; increasing linguistic dominance created by use of English or French as common business and political telecommunication languages; computer software written in one language (usually English). This concern cannot be totally separated from others such as national security or economics. It is frequently mentioned because of the added impetus it can give to these issues.

In addition to items mentioned above, language, political identity, etc., the whole question of information inundation in various media forms has been raised in Canada, in Europe and among the LDC's. The dominance of journalism from developed countries, the influence of the news services and major TV networks, and of U.S. motion pictures, are all drawn in larger letters when viewed in the context of new technological capabilities. This issue has been on a parallel track to many of the other IIF issues but as the press, TV and other publications providers increasingly share the same telecommunications and information processing facilities with business and other institutions like education and research, the lines of demarcation will start to collapse.

Summary of Recommendations

The U.S. policy and legal structure on privacy does not correspond to the European model. While this has been the subject of much international debate, to date there has been relatively little disturbance of American business interests overseas as a result of this incompatibility. Thus far, U.S. privacy policy has been effective in protecting the rights of American citizens, and there is no domestic reason for changing it at this time, especially in the absence of a better alternative. As further domestic and international requirements arise, legislative modification and judicial re-interpretation both at the state and federal levels may be necessary. Internationally, continued bilateral and multilateral efforts to clarify specific issues and solve individual cases will also be necessary.

The endorsement of the OECD guidelines by U.S. industry was never expected to produce guarantees of freedom from restriction for the endorsers by the signatory countries. Nonetheless, the endorsements are important international statements indicating the willingness of U.S. industry to cooperate on this key issue. The U.S. government should continue to support the guidelines as an important instrument.

The U.S. should continue to initiate and support worldwide efforts both bilaterally and multilaterally to ensure unrestricted flow and usage of information and information goods and services. In those rare instances where national security requirements (in the narrow sense) and protection of human rights make restrictions by our trading partners necessary, the U.S. should strive to ensure that these countries confine the application of these restrictions to the smallest possible number of circumstances. The U.S., itself, must also be equally cautious in its application of national security restrictions to avoid sending conflicting signals on the sincerity of our own commitment to unrestricted flow.

The U.S. should take a very strong stand against the commodity treatment of information. This principle has very fundamental implications for the creation of future trade barriers, both tariff and non-tariff. Special care must be taken in U.S. policy statements and position papers not to imply that such a classification for information is either acceptable or of no consequence to the U.S.

The impact of restrictive work rules and ergonomic standards is not yet fully understood in the international arenas dealing with information policy issues. U.S. representatives who participate in international information and labor conferences should be briefed on some of the special impacts work-rule modifications may have on information-intensive international industries.

Finally, the subjects of cultural and political integrity require special care for three reasons: 1) They are the issues least susceptible to any quantifiable analysis and measurement. Therefore, 2) they are also susceptible to rhetorical treatment and 3) they are often derivatives of other issues and are propelled by them, e.g., concerns for political integrity are