EDP ANALYZER

APRIL, 1978
VOL. 16, NO. 4

THE DEBATE ON TRANS-BORDER DATA FLOWS

Should the flow of data across national borders be controlled? Governments certainly have been trying for a long time to prevent the outflow of national security data. But how about less sensitive data, such as financial foreign exchange transactions, time sharing services, or airline reservation transactions that cross national boundaries? How about mailing lists that have the names and addresses of people in another country? The adherents of control say that they do not seek to constrain the flow of legitimate business data. But they *are* concerned when personal data on citizens of one country is stored in another country where little or no control of use exists. And they broaden their concern to include essentially *all* data applying to, say, a subsidiary company in one country where that data is stored and maintained at corporate headquarters in another country. The upshot is that some form of regulation of trans-border data flows (TBDF) is already starting to appear and is very likely to increase. This means that regulation will begin to impact international data processing, and possibly domestic data processing also. So keep your eye on this emerging area.

Should any trans-border data flows be controlled? If so, which ones and to what extent?

If one is concerned with business data processing, the tendency might be to almost dismiss these questions with an answer something like, "What a ridiculous idea; the flow of data is basic to international trade." But, as we will try to show in this report, the questions cannot be dismissed that casually. In fact, it appears to us as though a non-trivial amount of regulation will be imposed on trans-border data flows in, say, the next two to five years. So this is a subject in which many data processing executives should be interested.

This report was triggered by a symposium held in Vienna, Austria, late last September. The subject of the symposium was "trans-border data flows and the protection of privacy." The symposium was organized by the OECD and held in Vienna at the invitation of the Austrian Government, to coincide with the introduction of Austrian privacy legislation. It addressed problems raised by the rapid growth in volume of data crossing national boundaries on computer networks. Some of this is personal data, where protection of privacy is important. In addition, a number of people at the symposium felt that trans-border data flows *in general* must be considered, to protect the integrity and privacy of organizations, both governmental and industrial. Questions of national inter-dependence, cultural heritage, and national sovereignty are involved. Also, the question of non-tariff trade barriers was

evident, although not on the agenda.

Our report will deal with the subject from two viewpoints. For one thing, we will give our interpretive overview of what the symposium covered:

- The present situation
- What is the problem?
- How to solve the problem

Secondly, we will review some thoughts of other authors on this same symposium to help broaden the perspective on the subject. Since our views on the symposium are influenced by our feelings on government regulations in general, we have sought out other viewpoints in order to give a more balanced picture.

As will be seen from the "debate," this subject has wide ranging implications, for many types of organizations.

THE OECD SYMPOSIUM

The Organisation for Economic Co-operation and Development (OECD) is an international organization of 24 member countries, from Western Europe, North America, and the Pacific area. It is not a government organization, *per se*, is not a part of the United Nations, nor a part of the European Economic Community. Rather, it provides a forum for international co-operation, by holding conferences, symposia, committee meetings, and working group meetings, for formulating guidelines for policy making. The governments of the 24 member countries give considerable weight to OECD recommendations when drafting new legislation involving co-operation on international problems.

The OECD symposium on trans-border data flows and the protection of privacy was attended by about 250 people from some 20 countries. Among the attendees were representatives from 14 other international organizations, including the Council of Europe and the European Parliament. Papers and comments were presented in a number of languages, with simultaneous translation into the major languages. The proceedings of the symposium will be available from OECD (Reference 1).

We should mention that the OECD is not the only international organization working on this subject area. Others include UNESCO, the European Parliament, the Council of Europe, the European Community, the European Economic Community, and the Nordic Council. So the interest in the subject is quite widespread. Further, there is considerable exchange of information and ideas among these organizations.

As one of the speakers from the U.K. observed, the subject of the symposium is not a case of a problem that will go away nor a case where legislation can be emasculated. There is just too much attention being directed to it, on too broad a front, for it to "go away."

With this as a preamble, let us consider how the symposium speakers saw the present situation.

The present situation

We are pulling together the comments of many speakers that dealt with any given concept or idea. In general, we will not attempt to attribute specific comments to specific people in this overview. For the official record of the symposium, see Reference 1.

Actual trans-border data flows

As it turned out, symposium attendees could report only very limited factual data on today's trans-border data flows. Some studies had been made in Sweden, France, Germany, and the U.S. One multi-country study had just been commissioned, to be performed soon after the symposium.

The main point is: no one really knows what types of data, and in what amount, are actually flowing across national borders.

The *opinions* that we heard expressed at the symposium seemed to indicate the following (and no one there challenged the points).

Trans-border data flow is a very small percentage of total data flows on computer networks. Many local units of multi-national organizations apparently have become relatively independent of their parent companies, as far as their data processing is concerned. While this might hold in general, some multi-national companies have centralized their data processing in one or a few countries, including employee record processing.

Of the TBDFs that do exist, most seem to involve economic, financial, and administrative data. Not much has been detected of a purely personal nature—although international credit card transactions clearly are of this type and represent a significant volume. A study of the trans-border

flow of medical data concluded that the volume is low, apparently is not growing significantly, and does not yet warrant international regulation. (However, the Council of Europe is studying this area.) Where personal data does flow across borders, it generally deals with managers and executives who are being transferred to a unit in another country, one participant observed. Another participant disagreed somewhat, stating stating that some multi-national companies have sought to do *all* of their data processing at their headquarters.

Even though TBDF is a small percentage of total data flows, it has been growing rapidly. The symposium heard about a wide range of existing data flows, for airline reservations, banking, credit insurance, information services, and other applications. It should be recognized that these networks *do* carry personal data, in that transactions usually can be tied back to individuals. It is expected that such TBDFs will continue to grow rapidly and thus pose greater problems in the future.

In Sweden, one study found that several thousand Swedish companies were using time sharing services for their financial data processing, where the computers were located in other countries. Although no one else reported on a similar study, the impression was given that participants from countries other than Sweden felt that the same was true in their countries.

Logica, Ltd., of the U.K., has been commissioned by six Western European countries to study trans-border data flows in those countries. Some participants felt that no such study could get the needed data on a voluntary basis and that perhaps laws had to be enacted before the "real" data would become available. It will be interesting to see what success Logica had in collecting the desired data. (The U.S. Privacy Protection Study Commission, with powers of subpoena, was able to collect the data it needed—but its data did not apply to TBDF.)

Types of international networks

Since international computer networks are the "cause" of the problem addressed by the symposium, the characteristics of the two main types of networks were briefly considered. *Private* data networks carry most of today's TBDFs. *Public* data networks are just entering service nationally, and TBDF has hardly begun on them.

Individual organizations with private networks. An example of this type of network is the large, multi-national company that has plants in, say, 25 countries. It starts its international network with circuits leased from the national telecommunications agencies, to communicate with a few major plants in the nearest countries. It then gradually expands the network until it includes all plants. For each plant, communication services are selected that are appropriate to that plant's volume of traffic. So private networks are being designed and installed to meet the specific needs of each user organization, and serving only the units of that organization.

Joint use of private networks. Two such joint use networks were discussed, the SITA airline reservation network (which we discussed in our February 1975 report) and the SWIFT international banking network (mentioned briefly in our October 1977 report). While the number of such networks probably never will be large, because of legal restrictions on who can use them, nevertheless they represent a good amount of the total volume of today's TBDF traffic.

Public networks. The official telecommunications organizations, typically the governmental PTTs, are developing alternatives to these private data networks. The Nordic Data Network, serving all four Scandinavian countries, will go into operation next year. It will provide closed group service (which allows transmission between members of a group only, thus simulating a private network), the barring of incoming calls, the barring of outgoing calls (other than to members of a group), and so on. A representative of this network stated that the Swedish Data Inspection Board insisted that this network provide closed group service and the barring of all international calls.

Euronet is a packet switched network being developed by the government telecommunication agencies (PTTs) of the countries of Western Europe to provide direct access to bibliographic files of scientific, social, and economic information (information retrieval services). It also will be in operation next year. It may be used by the PTTs

for providing international linking of national data networks.

The subject of the symposium—the need for regulating trans-border data flows—was not discussed in terms of these networks. That is, there was no discussion of how easy or how difficult it might be to monitor each type of network, if TBDFs are regulated. One participant mentioned that a joint use private network had been used for sending "political" messages disguised as commercial messages. Also, there was no discussion of, say, likely differences in data security measures between public and private networks, or between networks that use cable, microwave, or satellite media.

Actual abuses

Very little information was presented at the symposium on detected abuses in TBDF, nor was there an attempt to define "abuse." One session chairman mentioned that the only abuses even casually discussed at the symposium were the ones that "everyone already knows about." He asked if anyone there had one or more new detected abuses to report; no one did. One other participant, an executive in an international time sharing company, said that he had never personally encountered a computer abuse during all of his years in the computer field.

The studies of the U. S. Privacy Protection Study Commission, while not concerned with TBDF, are of interest. One participant reported that at the beginning of the Commission's study, it was assumed that the study would find corporations maintaining large, sinister, and hidden files of personal data, used for manipulating the lives of the employees. What was actually found (remember that the Commission had subpoena powers, for digging deeply) was that essentially all companies kept just personal data needed for paying their employees, administering benefits, and providing government reports. Where evaluative information was kept, in general it applied just to senior management people. There was one exception noted. The study found that first line supervisors in companies tended to keep unauthorized, desk drawer files on subordinates. The information in these files was frequently obscure, irrelevant, or even slanderous.

The question of the types and frequency of abuses in TBDF was thus not clearly answered at the symposium. The subject area would have to be classified as "still largely unexplored."

Existing legislation

The Swedish Data Bank Law was enacted in 1973. It controls the handling of personal information in Sweden. But "privacy" in Sweden is different from that in other countries in some respects. For instance, the earnings of all individuals are public knowledge and available in local libraries; in most other countries, this information is considered personal and private. From the standpoint of TBDF, one example of the law's impact was cited. In this case, the Siemens Company in West Germany wanted to centralize all employee records for its worldwide operations in Germany. However, the Swedish Trade Unions objected to storing records on Swedish employees in Germany since Germany did not then have a privacy law in effect. So the Data Inspection Board denied the request. (The DIB *has* authorized a good amount of TBDF, we were told.)

The U. S. Privacy Act of 1974 mandates the principles of "fair information practices" be used by U. S. federal agencies. We discussed the application of this law in our November and December 1975 reports. The law set up the Privacy Protection Study Commission, which (among other things) was to study the need for similar legislation applying to the private sector. The Commission has completed its study and has recommended specific corrective legislation, not omnibus privacy legislation for the private sector. In addition, eight States have enacted privacy legislation—which, unfortunately, has not been too consistent with each other or with the federal law. In general, the U. S. private sector is not yet covered by privacy legislation, nor has the legislation paid attention to TBDF.

The Federal Republic of Germany has passed the Federal Data Protection Act of 1976, which went into effect at the beginning of this year. It holds for all personal information that is *stored* in Germany or in German territory, regardless of where those persons reside. It prevents the flow of personal information to countries that do not have similar laws with the same order of protection.

At the end of 1977, after the OECD symposium was held, France passed an omnibus privacy law applying to human persons. Extending the law to

cover legal persons was debated but this provision was omitted in the final law.

In addition, privacy protection laws are under consideration in most of the other OECD countries.

So far, there has been little "harmonization" of such privacy legislation. Each country (and in the U.S., each State) has pretty much gone its own way, even though each law has been based on the same concepts of fair information practices. One of the purposes of the symposium was to point out the need to harmonize such legislation, to avoid gaps, incompatibilities, and even contradictions in the enforcement and regulatory standards and procedures. Also, as mentioned earlier, some persons at the symposium hoped that it would recommend the need for legislation for controlling the trans-border flow of data on "legal" persons (e.g. companies).

What is the problem?

With TBDF representing only a small fraction of total computer network data flows, with every few abuses reported, and with most OECD countries moving ahead with privacy protection laws, the question must be asked: "What is all of the fuss about? What is the problem?

Let us begin this discussion of the problem area by describing briefly the fears that people at the symposium raised about TBDF.

The fears about TBDF

A good number of participants at the symposium saw several areas of potential threats due to differences in national privacy laws and the effect of these differences on the flow of data among countries.

International trade thwarted. While each privacy law currently in force is similar, each differs from the others for valid reasons (history, culture, etc.); this promises to be true for future privacy laws, too. These *differences* can and will act to inhibit the flow of legitimate business data in an undesirable manner. The best way to assure that international trade is not restricted improperly is for the various countries to agree on some minimum set of regulatory principles that apply to TBDF.

National laws circumvented. If large variations exist in the amount of privacy protection afforded by the several national laws, protection, like water, will tend to the lowest level. These variations would encourage organizations to store their data in the most permissive countries. In fact, it is quite possible that some countries would deliberately set up very permissive laws in order to attract "data storage and processing" business. Since data is so easily moved via computer networks, the idea of such data havens is not at all impractical.

So, say the adherents of control legislation, international cooperation is needed so as to support national privacy laws and to prevent the emergence of data havens. National legislation would have to be more restrictive in the absence of international co-operation.

Possible abuses. While most multi-national organizations might be using, and might continue to use, benign policies about personal data, the governments must be concerned about the few "bad" organizations. And in order to identify these "bad" organizatons, it is necessary to define "bad" behavior by way of the law.

Threat to national sovereignty. If data that is important to one country is stored and processed in another country, the national sovereignty of the first country can be jeopardized. Undesired disclosure of the data may occur, perhaps via search and seizure by the government of the second country or via system penetration by government or private parties. Access to this important data may be denied to people in the first country, due to strikes, actions of the local government, or other. The system may have been set up under a "friendly" government in the second country, but a new government might be much less friendly.

Double jeopardy. If national laws are in conflict or are contradictory, a business may find itself trapped into double jeopardy. In seeking to meet the laws of Country A, it violates the laws of Country B, and vice versa. Or even if the laws are not contradictory, the company may still find itself being penalized by both countries. For a company doing business in multiple countries, how does it determine which laws are to be followed for data that moves across the borders?

Potential trade barriers. It was pointed out that some countries might use their privacy laws as surreptitious trade barriers.

Threats to use of technology. Other participants, warning against "witch hunting" for imaginary abuses, said that TBDF regulations might well restrict the legitimate use of new technology.

These fears, it seems to us, were the ones most frequently raised at the symposium.

Since these fears were concerned with the flow of data across national borders, the next question to ask is: "What types of data are these people worried about?"

What types of data?

Several types of data were discussed at the symposium as possibly being candidates for TBDF regulation.

Personal data. Since the symposium dealt with "the protection of privacy," it would be expected that data relating to human persons would be singled out for attention.

However, it is sometimes quite difficult to determine if data is "personal" or not. One definition being used today is that if there is any way at all to tie a data record back to an individual person, then the whole record must be considered as personal data. For instance, a credit card transaction, since it includes the card holder's account number, must be considered personal data.

Some of the speakers were asked to define personal data. In general, they preferred not to try to do so.

Just as important, some of the participants wanted to broaden the scope of personal data so as to include data about "legal persons" (such as corporations). If the definition of personal data were enlarged in this manner, it would mean that information about organizations would have to be treated with the same care as information about individuals.

Non-personal data. Non-personal data includes economic data, financial data, statistical data, and so on that cannot be related to (a) a human person or (perhaps) to (b) a legal person.

The bulk of the data being transmitted between countries by most multi-national companies probably would fall under the "legal person" type of personal data plus non-personal data.

If significant penalties are imposed for violations of data transfer regulations, and if there were any question as to whether the data is personal or not, the responsible managers are probably going to be very cautious and classify the data as personal. This could have an effect on much international commerce.

Data sensitivity. There was a fair amount of discussion at the symposium on whether or not only the more sensitive types of personal data could be subjected to regulation. But the point was well made, we thought, that data is sensitive in context and not in the absolute. Generally, a person's address might be considered relatively insensitive and thus not subject to privacy protection; after all, the addresses of many people are published in telephone directories. But if the address of the person is a mental institution, it probably would be considered sensitive. And if the person were a possible target of terrorists, again the address would be sensitive.

In short, it is probable that no fixed rules could be set up that said such and such data items were not sensitive and thus need not be subject to regulation. There would be numerous exceptions to any such rules.

There was some discussion about whether it mattered where data is stored and processed. The time sharing service people, of course, argued that the location makes little or no difference. Somewhat surprisingly, we thought, someone from the banking industry agreed with this view. We cannot imagine, for instance, the Bank of England being willing to have all of its machine language records stored, and the processing of those records done, in some other country.

We do not want to give the impression that the bankers are unconcerned about this whole subject area. We gather that international banking is *very* concerned about the possible effects of TBDF regulation.

There was really no in-depth discussion at the symposium on the question: does it matter where information is stored and processed. As will be brought out later in this report, we suspect that it *does* matter.

However, the subject of the types of data that might be subject to regulation was discussed at some length. The consensus was that it would be

quite difficult to specify types of personal data that, in all cases, would be allowed to flow freely.

Confusion in problem definition

The two points just discussed—what are the fears and what types of data—may give the impression that the "problem" addressed by the symposium became reasonably well defined during the course of the discussions. Unfortunately, that was not the case.

Several speakers pointed out the confusions that existed in the problem definition. Briefly, these were the following.

What protection is being sought? Some participants seemed to be concerned solely with the protection of human personal information. Others assumed that the protection should "obviously" be extended to cover legal persons. Still others felt that the protection of national sovereignty was the most important issue. No concensus was solicited nor obtained on this point.

Can "privacy" and "sensitivity of data" be defined? Should they be defined? As we have indicated, there were material differences of opinion on the ability to define these value concepts and even on the need to define them.

Protection is being sought for what types of abuses? As indicated earlier, no new abuses in the use of personal information were related at the symposium. One speaker felt that it was ridiculous to try to protect against every conceivable abuse for which new technology provides an opportunity. At the other extreme were the participants who said they wanted to solve problems before they occurred.

Where do the greatest threats to privacy come from? Although not explicitly brought out very often, the underlying fears seemed to be directed at the large, multi-national corporations that might use personal information so as to manipulate their employees. But, said one speaker, do not the greatest threats to privacy come from public (governmental) data systems rather than from private ones? Also, are not inadvertent errors much more the cause for concern than deliberate actions, based on what has happened in the past? These questions were left hanging. In brief, there was no consensus at the symposium as to the sources of the greatest threats.

Is data to be considered a "product"? If data is considered as a product, it may then be subjected to many of the export and import controls to which products are subjected. With all of the problems involved in licensing the importation of physical products and then getting those products cleared through customs, is this desirable for data? Is it even feasible for data, what with high speed data transmission on international networks?

Who "owns" the data? Does an employee "own" all of the personal data about himself or herself in the employer's files—including data about skills developed during employment, training received, and so on? Or does the employer "own" the data? Or is there some type of joint ownership? This question was raised at the symposium but drew no response whatsoever.

Which of the issues raised at the symposium are more properly handled at the national level and which ones must be handled at the international level? There was no discussion that clearly differentiated the issues in this manner. In fact, some speakers advocated that new privacy laws be delayed awaiting the solution of TBDF problems, while other speakers said that national laws should not have to await the guidelines for TBDF questions.

What is the problem for which the regulation of TBDFs would be the solution? Some fears, ranging from threats to human privacy to the loss of national sovereignty, were expressed. The types of data that might have to be regulated were not agreed upon. No clear picture emerged of what protection is desired, against what abuses, by what national or international actions.

In short, the "problem" is not yet well defined (as is unfortunately the case in most other international problem areas).

How to solve the problem

The fact that the "problem" was not well defined did not deter the presentation of some alternative solutions. Each person presenting a solution was attempting to solve his concept of the problem, of course. As such, these solutions have real value, we think. The alternative solutions (should) force people to consider what problem each solution seeks to solve. So problem definition probably is aided by these proposed solutions.

Because there was no concensus on what the "problem" is, one would expect that the alterna-

tive solutions would have quite different goals. That is what occurred. Here is the gist, as we see it, of what was proposed.

What kind of regulation?

Most of the regulation of TBDF would have to be built into national laws. Before this can occur, agreement must be reached (through activities such as this symposium) on some minimum set of regulatory principles. In addition, some international sanctions may be found to be necessary, for types of (unnamed) abuses that cannot be handled adequately at the national level.

In addition to this minimum set of regulatory principles, the harmonization of existing privacy laws, and those close to enactment, must be realized. This will not be an easy task, it was pointed out. It is not a case of just drawing up a list of desired actions and then asking each nation to incorporate these into its privacy laws. There is a wide range of national attitudes in the various countries, reflecting cultural differences, that will cause such a list to be modified.

Even more important, this minimum set of regulatory principles must be based on an underlying philosophy. Two terms characterize the two main schools of thought on this philosophy: protection and correction.

For protective legislation. The advocates of this philosophy say that abuse problems should be solved before they occur, including ones that have not yet occurred because the technology is just now making them possible. It is not sufficient, say these people, to try to study what abuses are now taking place. First of all, it may well require that the new regulations be enacted before the abuses are flushed out. Secondly, technology is making new types of abuses possible and they should be prevented from happening.

For corrective legislation. The advocates of this philosophy say that the minimum set of regulatory principles should attempt to correct the worst of the abuses that are actually occurring. Omnibus preventive legislation tends to create problems where none previously existed, and fails to identify the underlying causes of problems that do exist. The end result is a poor solution to these existing problems. Omnibus preventive legislation may encourage organizations to comply with the letter, rather than the spirit, of the law. Further, omnibus preventive legislation holds the danger of "over-kill" and can have very serious effects on legitimate international trade.

The advocates of corrective legislation time and again urged that in-depth studies be conducted, to learn more about existing TBDFs and the abuses that are occurring. Legislation should then be directed at specific problems, they said.

This difference of opinion on "protection" versus "correction" was the most fundamental issue discussed in the symposium, in our opinion.

To give some idea of what principles *might* be adopted for TBDF regulation, the OECD pulled together, in a background paper for the symposium, some of the most significant guidelines excerpted from proposed or enacted laws. For one thing, records on human persons should not contain information on their race, opinions, political activities, trade union membership, medical condition, alcoholism, criminal offenses, confinement for mental disorders, discharge from the armed forces or forfeitures of civil rights. (Remember that TBDF regulation may require maintaining personal records in the same manner as required in the country of data origin.) Further, credit bureaus for citizens of a country may not be operated outside of its territory. Thirdly, restrictions will be placed on the use of personal data in advertising, direct mail, credit bureaus, insurance organizations, and others, both for use within the country and for transmission abroad.

(If principles such as these are proposed for inclusion in national privacy laws, in order to harmonize the various laws, such principles certainly will have an effect on domestic data processing.)

It is too early to say just what kind of TBDF regulation will evolve, but perhaps this discussion gives some idea of what is being considered.

Who should be regulated?

Trans-border data flows involve the transmission of data between different organizations, and/or between different components of the same organization, that are located in different countries. The functions of data collection, transmission, storage, processing, display, and eventual use will thus be spread out over multiple countries.

This being the case, if TBDF is to be regulated, which organization or organizational component must bear the prime responsibility? That is,

whose actions are to be regulated? The question gets more and more complicated as third-party organizations, such as service bureaus and telecommunication agencies, are brought into the picture.

One speaker, from the Computing Services Association of the U.K., proposed the concept of "beneficial user" and "processing agency" in order to unravel this problem. After his presentation, several other participants said that, in their studies, they had reached much the same conclusions.

The *beneficial user*, said this speaker, is that person or organization on whose behalf, and under whose direction, data processing work is done and who benefits from that data processing work. The *processing agency* is the organization that stores the records and performs the processing for the beneficial user. (It seems to us that these definitions should be enlarged to cover data transmission agencies also, although they are already either regulated or government owned.)

Under this concept, it is the beneficial user who should be the subject of the regulation of TBDF, said this speaker. If the use of data in a country must be licensed, then it is the beneficial user who should obtain the license. As for the processing agencies, at most they should be required to be certified, to attest that they do in fact meet satisfactory and relevant standards of security, privacy, and so on. These agencies may not necessarily be expected to know what data is being stored or transmitted, nor how it is being used.

Under this beneficial user concept, it matters not, said the speaker, whether the data processing is done by the data processing department of an organization or by an outside service bureau. In each case, the processing is being done by an agency. Further, that agency should have contracts with its users that spell out the responsibilities of each.

There was a good amount of discussion of this concept that we will not attempt to discuss in detail. One point concerned an international airline reservation system, where any agent with a terminal would be a beneficial user. How would the airline, which was the prime beneficial user, assume responsibility for data entered in its behalf by agents around the world? Also, what happens when governments serve subpoenas on processing agencies and demand access to records, without going through the beneficial users? The CSA spokesman indicated that this was a good example of where international co-operation could be very helpful. We expect to see and hear a lot more discussion of this concept. (For a copy of this paper, see Reference 8.)

The beneficial user concept was discussed primarily in terms of the *use* of data and the impact of privacy legislation on that use. Very little was said about its application to data transmission. As we said earlier, more attention must be paid to the role of public and private data networks in a regulated TBDF environment.

What is the meaning?

What is the real message of the OECD symposium in Vienna? Several authors have given their interpretation, including Pantages (Reference 5), Pipe (Reference 6), and Crawford (Reference 7). We think their views will help to give added perspective to our discussion.

Pantages singled out the remarks of Judge Jan Freese, Director General of the Swedish Data Inspection Board (and perhaps the moving force behind the OECD symposium). The proliferation of national privacy and data protection laws around the world offers potential problems for any organization that wishes to transmit data across borders. On the other hand, the uncontrolled flow of data across borders creates problems for the economy, society, and defense of a nation. Thus, from the standpoint of both the nations and the organizations that wish to transmit data across borders the regulation of such data flows is needed, said Freese.

(Pantages also reported on a survey she made of some 40 U.S. multi-national companies, to learn their opinions on this possible regulation. Over one-half of the people contacted were unaware of what is going on, she said. And of the rest, some believed that the new laws would have no effect on their operations. Interesting ! And disquieting!)

Pipe, who was a consultant to OECD in the organization of the symposium, pointed out that the symposium had only a limited mandate: to explore the main issues. No attempt was made to come to grips with certain of the "sensitive" issues, such as using TBDF regulation as a non-tariff trade barrier.

Another sensitive issue not discussed, said Pipe, was the question of protecting records stored in another country against seizure by the government of that country. He then cited a relevant instance involving Donn Parker, well known for his work on computer abuse. We checked with Parker about this instance.

Several years back, said Parker, he wrote an editorial for *The New York Times* in which he mentioned some Swiss banking data being entered into a U.S. time sharing service from terminals in Switzerland. Wasn't it interesting, he observed in the editorial, that those banking records were protected from subpoena in Switzerland but could be subject to subpoena in the U.S. Sometime after the editorial appeared, Parker was visited by two representatives of the U.S. Internal Revenue Service, who wanted more of his thoughts on that matter.

Could such records be seized by the U.S. government? We have heard of no such instances and Parker indicated to us that he had not heard of any such instances either. If, in this example, Swiss banking records were seized, would this be a violation of Swiss sovereignty?

Several comments that we heard at the symposium, plus others we have heard since, have given us the impression that such seizure would not be out of the question in almost *any* country, given the right conditions. Unless international agreements are adopted to the contrary, we think it would be wise to assume that records stored in another country are subject to seizure by the government of that country. (For many users, of course, this might be an almost meaningless threat.)

Crawford, one of the key U.S. government delegates to the symposium, reported that one of the main results of the meeting was to expose many Americans to strongly held European ideas on international data processing. The Americans could see the European determination to harness computer technology to humane purposes, and to serve European ends.

The Europeans exhibited a sense of urgency that was not shared by the Americans, said Crawford. With the imminent adoption of privacy laws in many countries, they want action now. The Americans urged a more deliberative approach, careful studies, and better problem definition—causing frustrations among some Europeans. Many Europeans view privacy legislation as a paramount human right, and ask the Americans, "How much evidence do you need to justify an action that is morally sanctioned?" To this, the Americans reply, says Crawford, "Enough to show that the action does not have immoral results."

Several authors point out that, while human privacy was at the center of the discussion, other uses for data protection were clearly in the background. One such use is to constrain the rapid growth of U.S.-based time sharing services and information services in Europe. Another use would be to constrain somewhat the control that multinational companies have over their foreign subsidiaries (and thus possibly constrain the spread of these multi-nationals). And another possible use of data protection would be to limit somewhat the amount of advertising that can be directed to residents of other countries. Thus, international trade *can* be affected by TBDF regulation.

Overview of the problem area

Eger (Reference 3) points out that the concern with TBDF really is just part of a much larger issue—an issue that Eger calls "the information war." He reviews some main points made at the OECD symposium. Not only do Sweden and Germany now restrict the flow of personal data across their borders but also Belgium and France reportedly are making it a *criminal* offense to transmit some types of data. And Switzerland is considering prohibiting all electronic transmission of data across their borders, he says.

Then Eger goes on to point out that these restrictions on the flow of data are just part of a broader attack on all information flows. A growing number of countries have imposed restrictions on the use of U.S. television programs, films, and magazines. International sanctions are being sought to prevent satellite broadcasts into other countries. Some developing countries apparently are rejecting the use of U.S. technology for education and entertainment purposes. And *Time* magazine has either been banned or taxed out of existence in 18 countries, says Eger.

As we pointed out earlier in this report, no one really knows just how much trans-border data flow and information flow actually are occurring. Yes, some studies have been made but it is not clear how accurate or how complete their find-

ings are. Countries that are worried about U.S. domination of their economies are deciding that they want to find out just what the situation is. And it may take TBDF regulations in order to find out, some think.

There is some evidence to support this belief. Judge Freese, in his presentation at the symposium, cited a Swedish Data Inspection Board study of Nordic TBDF. The DIB files showed large data flows between Sweden and the other three Nordic countries. To learn more about these data flows, the DIB sent requests for information to organizations in these other countries—but none of those organizations could be forced to answer. Some 15 to 20 requests were made to organizations in one country. Not all responded, and of those that did, some did not tell the truth. About 400 requests were made to each of the other two countries, and less than 20 replies were received from each. Only through laws that regulate TBDF will the actual facts be found, said Freese.

So it is quite possible that restrictions on the overall flow of information, as well as on the flow of some types of business data, will be widely adopted in the not distant future. And the restrictions will be used by the various countries to clearly identify the information flows and data flows that do exist.

As mentioned above, Pantages reported that over one-half of the companies she contacted were not aware of what is happening, and some of the rest felt that the new laws would not affect their operations. Let us consider one example of what can happen.

A specific example

S. N. McRae was the chief executive for the *Reader's Digest* in Sweden whent he new Data Act went into effect. In Reference 4, he vividly describes his experience and his view of that experience.

The *Reader's Digest* had developed, over a period of years and from numerous publicly available sources, a mailing list of essentially all households in Sweden. The company preferred to develop and maintain the list in-house, rather than rent the lists of others, for a number of reasons. For one thing, they wanted to match their promotional list against their subscriber list, so as not to solicit new subscriptions from subscribers. For another thing, they wanted to indicate which promotional mailings had been made to which households. And there were additional similar reasons for wanting their own in-house Swedish list, to be maintained at the company's processing center (not in Sweden).

But the Data Inspection Board objected to this *Reader's Digest* list because of its sheer size and the fact that it was being maintained outside of Sweden. Instead, the DIB proposed that it set up a Swedish central list that others could rent. The DIB's motives were clearly those of self-interest, said McRae.

A reply to McRae was prepared by Judge Freese, Director General of the DIB, for publication in *Computing Europe;* he sent us a copy of his reply. Sweden is probably one of the most open countries, he said; everyone has guaranteed access to all public documents. This includes access to public information stored in computer systems. Any private company could legally load its files with lots of personal information, very cheaply. The *Reader's Digest* used such publicly available information for its files, said Freese.

But the DIB wants to treat all companies alike, he continued. If the *Reader's Digest* could set up such massive files of the citizenry, so could hundreds or thousands of other companies. And the DIB did not like *that* idea at all. Questions of personal privacy and even national defense arose. So Sweden amended its Data Act to say that permission to set up or maintain a personal register (list) which includes a considerable part of the population may be granted, in general, *only* if the data subjects are members, employees, or clients of the list owner and are willing to be on the list.

(This would seem to threaten much of the advertising and promotion that is performed outside of Sweden and directed at specific Swedish data subjects, if we interpret it correctly, since "a considerable part of the population" is so ambiguous. If so, this would appear to be a rather extreme restriction on international trade.)

Thus there are two sides to this argument—which, we think, lies at the heart of "the debate on trans-border data flows." The *Reader's Digest* conducts what we consider to be a very legitimate and effective direct mail solicitation of subscriptions and sales of other products. Due to the wide appeal of the magazine and its other products, it is economically feasible for the company to send mailings to large segments of population in many

countries, as they do in the U.S.

The DIB, on the other hand, does not want to see a proliferation of huge lists on Swedish citizens that are set up and maintained outside of Sweden and thus outside of their control. This, too, seems like a legitimate desire.

This is just one example of a trans-border data flow that has been brought into the limelight by the Swedish Data Act. As privacy laws are passed in other countries, the number of such cases—of what have been legitimate business uses of data that are now denied by the governments—will surely grow. We suspect that *many* firms that do business internationally will find themselves at odds with the new privacy laws, and for reasons that they may feel have nothing to do with personal privacy.

We are not saying that such problems cannot be rationalized. The solutions may involve higher expenses, although this will not necessarily be the case, what with the rapid improvements in distributed system technology. What we are saying is that, at the least, many companies will find that they have to change their ways of doing business in order to comply with the privacy laws in the countries in which they operate. And some currently legitimate international trade may suffer.

Even greater troubles probably will arise if the privacy laws of the different countries have widely differing (and sometimes conflicting) requirements to be met. That is what some advocates of TBDF regulation are trying to avoid.

What is happening?

All of the people that we have talked to on this subject, and all of the articles we have read, agree on one main point—privacy laws will be enacted in *many* countries in the not distant future. The next two to three years will see numerous such enactments because the subject is politically popular. So the problem of conflicting laws and their effect on international trade is not something for the far future; it is here now, today.

What is being done to alleviate these problems? H. P. Gassman, of the OECD, in a letter to us, has summarized the main present efforts. Now that the French privacy law has been enacted, there are three European countries with such laws— Sweden, West Germany, and France. Further, all three of these laws apply to the handling of personal information on human persons; legal persons are not (yet) covered.

The Council of Europe is working on drafting an international Convention (agreement) to harmonize the existing privacy laws, and those to be enacted in the future, on the handling of trans-border flows of personal data. The OECD also may help to produce such guidelines. While this agreement would pertain mainly to European countries, non-European countries (such as the U.S.) may choose to adhere to the guidelines, he says.

Pantages (Reference 5) says that these developments—the privacy laws and the international agreements—are happening faster than the U.S. expected. The Council of Europe's draft agreement is scheduled to be completed late this year and may be ratified by member countries during 1979 and 1980.

Further, says Gassmann, the European Community has launched a two year study to investigate the flow of non-personal data.

Pipe (Reference 6) mentions some restrictions that have already been placed on TBDF by the governments of Australia, Canada, and Japan, in addition to the regulations imposed by the privacy laws of Sweden, Germany, and France.

So if anyone thinks that the regulation of trans-border data flows will not occur soon or will not affect international trade, such a person is in for a shock, we believe.

The U.S. *is* waking up to this development and starting to move. People at the Departments of State and Commerce have been carrying most of the burden up to now. But now Congress has investigations underway, in both the House and the Senate. A U.S. Interagency Task Force on TBDF has been organized. The National Security Council has begun an investigation. The American Federation of Information Processing Societies (AFIPS) has organized a panel on TBDF to provide information to government agencies in the subject area.

So we think you will be hearing more and more about this subject.

What is proposed

What might the draft of the international agreement, being worked on by the Council of Europe, contain? At this point, any answer would be conjecture. In addition to the points raised in

the OECD background paper, which we mentioned earlier, here are the thoughts of a prime mover for TBDF regulation.

Judge Jan Freese of the Swedish Data Inspection Board, in a letter to us, said the following. "My philosophy is rather simple. I realize that many nations will legislate in the field of computers and privacy. They have to do so, as Sweden did, because of national reasons. Because of very big differences in history, tradition, and legislation, none of the enacted privacy laws (Sweden, Germany, France), or expected laws, will be a copy of any of the others. Already this is a threat against international trade. Therefore, I want to solve problems before they occur."

"In order to keep the flow of information free, I realize that we need to regulate it. This is a paradox. I even believe that such regulation, through international agreement, should cover non-personal data. If we do so, it will not be easy to stop the existing free flow of information, since other nations will have this international agreement to point to.

"Of course, such an international agreement will have to be rather small in scope, covering not much more than the six principles I gave in my OECD paper. But the agreement should cover enough to make us feel safe in using the trans-border flow of data."

Here are the six (protective) principles that Freese feels will be sufficient for allowing the continued free flow of information and at the same time for protecting the rights of individuals, companies, and nations.

First, information shall not be divulged nor used for any purpose other than has been decided in its country of origin.

Second, persons having legitimate access to this information shall be obliged to observe its secrecy.

Third, unauthorized access to information, including its alteration, damage, or destruction, shall be subject to legal penalties.

Fourth, reasonable security measures shall be used to protect the information.

Fifth, reliable and continuous movement of such information shall be assured.

Sixth, in the case of personal information, individuals shall have the right of inspection, unless specifically denied by law.

At first glance, these principles do not seem unreasonable. But their reasonableness (or not) can be determined only as they begin to be interpreted in a number of specific instances. Note that they probably can be interpreted so as to cut off some existing data flows, such as the *Reader's Digest* mailing list application.

This, then, is the "debate" on trans-border data flow, as we see it. We hope we have succeeded in giving a fair treatment to both sides of the debate. It is no longer a question of *whether* to control such flows; things have progressed much too far for that. Instead, the questions to be debated are *which flows* and *how much control.*

Regulation is edging further into the data processing field.

REFERENCES

1. *Proceedings of OECD Symposium on Transborder Data Flows and the Protection of Privacy, September 1977;* publication scheduled for this month, price not yet known. For information, write OECD, 2 rue Andre-Pascal, 75775 Paris Cedex 16, France; in U.S., write OECD Publication Center, 1750 Pennsylvania Avenue, N.W., Washington, D.C. 20006.
2. To communicate with OECD on this subject, write to Directorate for Science, Technology and Industry, OECD, at the above Paris address.
3. Eger, John M., "The Coming 'Information War'," *The Washington Post,* Washington, D.C.; January 15, 1978.
4. McRae, S. N., "The dangers of bureaucratic data laws," *Computing Europe* (76 Dean Street, London W1A 1BU, U.K.), November 17, 1977; page 11 (Letters to the Editor).
5. Pantages, Angeline, "Is the world building data barriers?" *Datamation* (1801 S. LaCienega Blvd., Los Angeles, Calif. 90035); December 1977, p. 90ff; price $3.
6. Pipe, G. R., "Transnational data issues dwarf privacy," article prepared for publication in *Computing Europe.* For a copy, write the author at International Business Action Centre b.v., Geuzenstraat 32, Amsterdam, Netherlands.
7. Crawford, Morris, "The Vienna Symposium," unpublished report. For a copy, write to the author who is Deputy Director, Office of Bilateral and Multilateral S&T Programs, U.S. Department of State, Washington, D.C. 20520. For U.S. readers, we suggest that if you have any thoughts, suggestions, or comments on the subjects of trans-border data flows that you would like to have considered, send them to Mr. Crawford.
8. Benjamin, Alan A., "Privacy and Computers," paper presented at OECD Symposium, Reference 1. For a copy of this paper, write Computing Services Association, Craven House, 121 Kingsway, London WC2B 6PG, U.K.; price 1.

It is estimated that less than twenty percent of today's mechanized data is stored in data bases, under the control of data base management systems. But the rapid growth in sales of* DBMS *and related software (such as data dictionaries) leads one to believe that in the next few years, this percentage figure will be much higher. So conversions to the data base environment will be occurring much more rapidly, we think. In addition, organizations that are using* DBMS *will be converting to new* DBMS. *Next month, we will discuss "planning for* DBMS *conversions," based on two working conferences on this subject.

SUBJECTS COVERED BY EDP ANALYZER IN PRIOR YEARS

1975 (Volume 13)

Number

1. Progress Toward International Data Networks
2. Soon: Public Packet Switched Networks
3. The Internal Auditor and the Computer
4. Improvements in Man/Machine Interfacing
5. "Are We Doing the Right Things?"
6. "Are We Doing Things Right?"
7. "Do We Have the Right Resources?"
8. The Benefits of Standard Practices
9. Progress Toward Easier Programming
10. The New Interactive Search Systems
11. The Debate on Information Privacy: Part 1
12. The Debate on Information Privacy: Part 2

1976 (Volume 14)

Number

1. Planning for Multi-national Data Processing
2. Staff Training on the Multi-national Scene
3. Professionalism: Coming or Not?
4. Integrity and Security of Personal Data
5. APL and Decision Support Systems
6. Distributed Data Systems
7. Network Structures for Distributed Systems
8. Bringing Women into Computing Management
9. Project Management Systems
10. Distributed Systems and the End User
11. Recovery in Data Base Systems
12. Toward the Better Management of Data

1977 (Volume 15)

Number

1. The Arrival of Common Systems
2. Word Processing: Part 1
3. Word Processing: Part 2
4. Computer Message Systems
5. Computer Services for Small Sites
6. The Importance of EDP Audit and Control
7. Getting the Requirements Right
8. Managing Staff Retention and Turnover
9. Making Use of Remote Computing Services
10. The Impact of Corporate EFT
11. Using Some New Programming Techniques
12. Progress in Project Management

1978 (Volume 16)

Number

1. Installing a Data Dictionary
2. Progress in Software Engineering: Part 1
3. Progress in Software Engineering: Part 2
4. The Debate on Trans-border Data Flows

(List of subjects prior to 1975 sent upon request)

PRICE SCHEDULE

The annual subscription price for EDP ANALYZER is $48. The two year price is $88 and the three year price is $120; postpaid surface delivery to the U.S., Canada, and Mexico. (Optional air mail delivery to Canada and Mexico available at extra cost.)

Subscriptions to other countries are: One year $60, two years, $112, and three years $156. These prices include AIR MAIL postage. All prices in U.S. dollars.

Attractive binders for holding 12 issues of EDP ANALYZER are available at $6.25. Californians please add 38¢ sales tax.

Because of the continuing demand for back issues, all previous reports are available. Price: $6 each (for U.S., Canada, and Mexico), and $7 elsewhere; includes air mail postage.

Reduced rates are in effect for multiple subscriptions and for multiple copies of back issues. Please write for rates.

Subscription agency orders limited to single copy, one-, two-, and three-year subscriptions only.

Send your order and check to:
EDP ANALYZER
Subscription Office
925 Anza Avenue
Vista, California 92083
Phone: (714) 724-3233

Send editorial correspondence to:
EDP ANALYZER
Editorial Office
925 Anza Avenue
Vista, California 92083
Phone: (714) 724-5900

Name_____

Company _____

Address _____

City, State, ZIP Code_____