There's Trouble in the Air over Transborder Data Flow

The integration of computers with modern communication systems has made it possible to transmit massive amounts of data worldwide relatively cheaply. The argument can be made that computer-aided communications makes possible the efficient operations of multinational corporations and financial institutions. The United States has been a major begetter of the new technology and maintains a dominant position in utilizing it. The economic and social implications of this dominance are a source of increasing tension between the United States and other countries, particularly those in Western Europe.

A focus of this tension is an elemental fact of data processing that once data goes into a computer, it is difficult to ensure that only those who should have access to them actually will. It is not surprising, therefore, that the new technology has given rise to efforts by governments to protect national security and the privacy of their citizens.

In the United States, perhaps because of a mistrust of government which is part of a hangover from Watergate, the emphasis has been on protecting citizens against government collection and storage of personal data without the knowledge of the individuals involved. In Europe, the focus currently is on regulating the flow of data across national frontiers, a traffic known in the data processing trade as "transborder data flow."

Several European countries have passed laws specifying what sort of information may be collected, stored, and transmitted by data processing systems and under what conditions. Substantial penalties have been decreed for transgressors. The full implications of these laws are still far from clear, but critics in this country charge that the effect and, in fact, the intention of the legislation is to curb American dominance in information technology and, in particular, to erect barriers to the activities of U.S.-based multinational corporations.

These critics see a hypothetical future in which corporations operating in Europe would not be permitted to transmit personal data on their own employees to the United States. The flow of scientific and technical information could also be inhibited, as, for example, in the case of American pharmaceutical companies which might be prohibited from transmitting results of drug testing involving humans.

So far, too few cases have been dealt with under the new laws to furnish reliable precedents. A French law, for example, has a 2-year transition period before coming into full force. Some restrictive decisions have been issued in Sweden. The Swedish Data Inspection Board, for example, denied permission to a Germany company, Siemens, to transmit data on its Swedish employees for processing in Germany: *Reader's Digest* was told it could not carry out a plan to process abroad a list of the names of 3.5 million Swedish citizens targeted for a mass mailing. But most informed observers caution that no sweeping conclusions should be drawn yet.

A Free-Trade Issue?

The controversy over transborder data flow is sometimes portrayed as essentially an economic rivalry, with the United States espousing a free flow of information and cast in the "free trader" role. By this analysis, the Europeans are the "protectionists." Such an interpretation is at least oversimplified.

First, all but the most cynical of American critics concede that the European concern about privacy—the European term is "data protection"—is genuine. Recollections of World War II are not yet extinguished on the continent, and there is a recognition that information about a person's religious or political attitudes could literally prove fatal. And there is concern that personal information in data banks, especially in other countries, could be misused and that economic information stored abroad could also be utilized in damaging ways.

It is also true, however, that information technology is perceived in Europe as not just another technology. And Europeans share a conviction that information technology is profoundly changing the workings of industrial society and are convinced that a given country will have little chance to control its own destiny unless it develops a measure of self-sufficiency in the new technology.

Evidence of the European view is found in rather pure form in a recent report to French President Valery Giscard d'Estaing on the impact of data processing on French society and on possible ways to develop and control it. It is called the Nora report for Simon Nora, Inspector General of the Ministry of Finance under whose direction the report was prepared.

The report puts the problem in the context of the long-term societal crisis caused by industrialization and urbanization. France is portrayed as facing a series of challenges which could deprive the country of the ability to determine its destiny. The "computerization of society" is identified as a key issue which could either worsen or help to solve the crisis. The stakes riding on information technology are described as nothing less than the country's "economic balance, the 'social consensus' and national independence."

The linking of computers in networks and their interconnection with telecommunications—the neologism "telematics" is coined to describe the union—is seen as changing the organization of society and requiring new policies to meet international conditions. The report goes on to say that "changes in economic and social structures can only be brought about if France can escape from the excessive pressures of foreign governments or groups whose objectives may stand in the way of her own ambitions."

Telematics threatens sovereignty by encroaching on traditional government powers over communications. The report cites as an example, and the choice is hardly accidental, the transformation of IBM from simply a "manufacturer of machines" to a "telecommunications administrator" when it sets up a telecommunications network.

In the national interest, the report says, the government should make "unrestricted use of the decree" to support companies which provide computer-related services, intervene in research, bolster the semiconductor industry, and encourage the national manufacture of large computers.

All of this follows the French penchant for sociological analysis of technological change and for providing an elaborately reasoned theoretical basis for action. And it reflects an attitude rather than policy. Nonetheless, the report expresses a view toward information technology on the part of European opinion-makers which cannot but have implications for the new data protection laws.

These laws, it should be emphasized, deal principally with protection of data

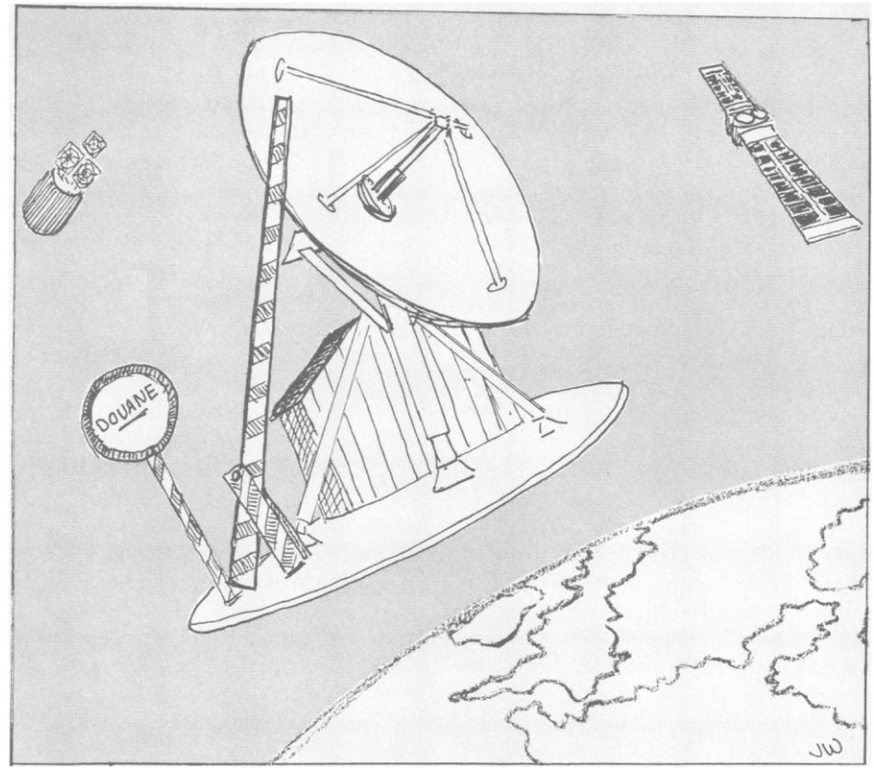
0036-8075/78/1006-0029$00.75/0

domestically and only secondarily and often indirectly with the transmission of data outside the country. The first data protection law at any level of government seems to have been enacted in the West German state of Hesse in 1970 and the first national law in Sweden in 1973. Laws in Germany and France followed and, more recently, Norway and Denmark. Other European countries are at various stages of the law-making process.

The French law, passed by parliament early this year, has attracted particular attention in this country, perhaps because the French have been the most vocal critics of American economic influence in Europe. The French law is typical of the national laws in establishing a board with extensive powers to administer the act. In France it is called the National Commission for Data Processing and Freedom. The law requires all name-linked data processing systems to be registered with the commission. Descriptions of data in each system, identification of persons responsible for data processing, and information on the uses to which the data will be put must be filed. Arrangements for individuals to have access to data about themselves are required and limits on the time data are to be kept are set. Penalties for infractions for some provisions can be as high as 5 years in jail or fines of up to $400,000. One provision which obviously affects foreign firms is that requiring the system operator to state whether personal data are being sent out of France.

A crucial issue is whether the laws will apply not only to physical persons, as the legalese puts it, but to legal persons, which include corporations. If legal persons were included, a corporation might have to open its files, for example, to competitors or clients mentioned in their communications. The French law in an early draft included legal persons. The provision would have affected domestic business and industry as well as international operations, and French big business, apparently led by IBM, exerted strong pressure on parliament to limit the law to physical persons. The campaign was successful. The broader definition, however, apparently applies in the Norwegian and Danish versions and is implanted in bills being considered in Austria and Luxembourg. And French officials have indicated that the matter may well be reconsidered in France.

While national laws in Europe follow similar lines they are by no means uniform. As a consequence, an effort is being made in the Council of Europe to fashion a data protection convention to



"harmonize" the disparate national laws and promote as free a flow of data as possible. While this may facilitate transmission of data in Europe it could leave the United States as odd state out.

The United States is not a member of the Council of Europe and, although it has been invited to send observers to meetings of the drafting group, has not taken a position on the convention. There is a possibility that the Council will call an international conference to open the treaty to nonmember states when it is completed. However, there is little likelihood that the United States would become a signatory with all that that implies.

A major problem is that the treaty seems sure to contain provisions inconsistent with U.S. law as it is now and is likely to develop. Basic U.S. law in the field is the Privacy Act of 1974 which applies in rather specific ways to the privacy of individuals in respect to government records.

Plenty of bills now percolating in Congress and state legislatures deal with privacy issues, but, by and large, these extend protection incrementally in specific, closely defined situations. The European approach, in contrast, is an "omnibus" one extending umbrella protection generally. Another difference is that European laws apply to automatically processed data only, while U.S. law makes no distinctions as to how information is handled.

Also important, the Council of Europe draft is likely to follow the national laws in prescribing creation of a fairly powerful data protection bureaucracy. Sentiment in this country currently is running against regulation and regulatory agencies with intrusive powers.

Parallel to the Council of Europe effort is an initiative by the Organization for European Cooperation and Development (OECD) to fashion a supplement to the council treaty which some backers hope will serve as an alternative. OECD includes Australia, Canada, Japan, and the United States as members as well as the Western European nations. The OECD is seeking to produce a voluntary, nonbinding international agreement on data protection. One objective is to devise a set of guidelines to which nations not having national privacy laws can subscribe and thereby satisfy the demands for reciprocal protection by countries which do have such laws.

Cassandras in the computer industry in this country foresee a situation in which European countries with data protection laws would prohibit companies operating within their borders to transmit data to the United States because their citizens would not have similar protection here. At present, even the limited U.S. privacy laws apply only to U.S. citizens and not to citizens of other countries.

There is considerable disagreement over whether European countries will move, so to speak, to embargo transmission of personal data to the United

States. There is a similar division on the possibility that the Europeans will impose nontariff barriers such as licenses and taxes on information operations which would fall heavily on U.S.-based companies.

The picture is likely to be clearer when the Council of Europe draft is finished—possibly at the end of the year—and the OECD guidelines completed. The OECD is aiming to have its final draft by next summer. If accommodation cannot be reached on reciprocity in data protection, there could be trouble.

State and Commerce department officials in this country have been negotiating on the transborder data flow issues, with American computer and software industries and their trade associations providing advice and, for the most part, urging the government to take a firm line.

Some edginess has developed in the relationship. Invitations from government to industry to provide information on transborder data flow restrictions have produced few citations of chapter and verse. This may not mean, however, that companies operating abroad have felt no pressure. As one government official said, "If you ask the government to help you, the biggest risk you run is that you may get it." What he meant was that intervention by U.S. officials may offend host country officials and prejudice future negotiations for the company. In addition, some companies shy away from confiding sensitive information to the U.S. government which, in some instances, has been known to slip up in protecting that kind of privacy.

The transborder data flow controversy has another major dimension. Less developed countries (LDC's) complain that the industrial nations, especially the United States, have kept the LDC's in a state of information dependence both by pricing and contracting policies on computers and related equipment and by denying them access to the technology which would allow them to establish their own information technology base.

The grievance is linked both to the LDC's discontent over technology transfer in general and to a broad set of issues which they regard as collectively constituting "information colonialism." The LDC's see Western global domination of news gathering and dissemination and control of communications networks as blocking economic development and threatening political and cultural self-determination in the LDC's (*Science*, 11 August 1978).

Unesco has provided a forum for the LDC's to develop their case, and sentiment for collective action by them to apply pressure on industrial nations to meet LDC needs has gathered some momentum. At a recent meeting of the Intergovernmental Bureau for Information in Spain, for example, some African nations sought to lay the groundwork for a regional computer industry. And discussion of applying of direct pressure on the industrial nations by restricting the flow of data across LDC borders was serious enough for delegates to vote a formal study of this strategy.

For the U.S. government, transborder data flow issues present complex problems for international negotiation. Existing U.S. domestic laws affecting data protection afford negotiators little room for maneuver and Congress has not assigned a high priority to action on privacy questions either domestic or international. The importance to the U.S. economy of the information technology industry here maintaining its remarkable momentum is at last winning wider recognition. And the transborder data flow question will provide an important test of American ingenuity and determination for both industry and government.

At the same time the United States can hardly ignore the fact that European nations, and Canada perhaps even more, regard what they see as an information technology gap as a threat not simply to national pride but to national survival. And U.S. relations with LDC's increasingly center on the American control of technology which the LDC's both resent and wish to share. U.S. diplomacy, to put it briefly, then must learn to deal better with the difficult fact that, to update Francis Bacon, information is power.

—JOHN WALSH

"Radwastes": Leading Policy Role Recommended for Science Adviser

The radioactive waste management issue arouses high controversy, but an ad hoc "radwaste" discussion group drawn from industrial, environmental, and academic circles is demonstrating that a surprising degree of consensus is possible at least on one important point. It is that federal policymaking in the radwaste field has lacked credibility and effectiveness under the leadership of the Department of Energy (DOE) and should be reassigned, at least temporarily, to the science adviser in the Executive Office of the President.

The group is pushing this recommendation hard despite the fact that it is strongly opposed by science adviser Frank Press as well as by John M. Deutch, DOE's director of energy research and head of the Interagency Review Group (IRG) on waste management established last March under a presidential directive.

The radwaste discussion group was put together by Robert W. Craig, president of the Keystone Center for Continuing Education at Keystone, Colorado, and former head of the Aspen Institute for Humanistic Studies. Craig, who has had a long-standing interest in the rad-waste problem, invited about 15 persons to take part in the group's first 2-day meeting, held at Keystone in August.

They included some prominent industry figures, most notably Alexander Trowbridge, Jr., vice chairman of the board of the Allied Chemical Corporation (and a former Secretary of Commerce), and James Buckham, president of Allied/General Nuclear Services; also present were a number of academicians including Dorothy Zinberg and Irwin Bupp of Harvard and Charles Hollister of the Woods Hole Oceanographic Institution, together with two environmentalists prominently involved with radwaste issues, Terry R. Lash of the Natural Resources Defense Council and Peter Montague of the Southwest Research and Information Center in Albuquerque, New Mexico.

Members of the group wasted little time arguing over their differences and, in an amicable manner, got down to discussing what could be done to move radwaste policymaking forward as a matter critical to the survival of the nuclear industry. The upshot of this August meet-

0036-8075/78/1006-0032$00.50/0