UIC John Marshall Journal of Information Technology & Privacy Law

Volume 2
Issue 1 *Computer/Law Journal - 1980*

Article 33

1980

Book Review: Computer Networks and Data Protection Law, 2 Computer L.J. 903 (1980)

Fred M. Greguras

BOOK REVIEW

COMPUTER NETWORKS AND DATA PROTECTION LAW

(A Special Issue of Computer Networks—The International Journal of Distributed Information)

Awareness, farsightedness and problem-solving of the interwoven issues involved in data protection laws will be enhanced by the reading of *Computer Networks and Data Protection Law*, the June 1979 special issue of COMPUTER NETWORKS. The purpose of the special issue is to provide an international overview of the status and implications of data protection laws and to predict what the future holds.

The technological achievements of the 1970s have been enormous; the 1980s promise to bring even greater challenges and accomplishments. The information processing industry is becoming a major national asset of many nations. The absence of such an industry or the lack of control over it is of increasing concern to other countries, particularly Third World nations.

The United States' leadership in the international marketplace, some would call it dominance, is diminishing. Challenges in technological developments are mounting from Japan and Western Europe. In other nations with a more farsighted view of the emerging international marketplace, technological innovations are directly subsidized by the government and/or are encouraged indirectly by such means as tax incentives. In contrast, the United States government appears to view the development of technology as purely a domestic matter, to be stimulated by the traditional forces of competition. Generally, the same limitations imposed on business enterprises seeking customers in the domestic market are enforced as United States business competes in the international marketplace.

Complicating this situation for the information processing industry in the United States and elsewhere is the growing number of what have been labeled data protection laws. These laws are

grounded on the protection of individual privacy, but are also, or have the potential for being, expressions of economic protectionism and nationalism. If advanced technology cannot be utilized because international marketplaces are closed by direct or indirect means, the incentives for technological innovation and other business development will be limited. Further, the internal economic implications for the United States and other nations will not be restricted to a single industry. Indeed, the impact will be felt by users of information processing equipment and communications networks and, by a ripple effect, in other industries. Some multinational corporations assert that this impact is already being felt. Considered independently, the inconsistencies of data protection laws may not appear to be restrictive but the aggregated compliance requirements could present insurmountable technological obstacles and/or severe economic implications. An on-going empirical study being conducted by the Link Consulting Group and the Transnational Data Reporting Service could produce the first quantifications of this impact.

The two prominent co-editors of the special issue of COMPUTER NETWORKS, Fritz Hondius and Paul Sieghart, have assembled an outstanding group of authors for this compilation of views and facts concerning data protection laws. The scope of the issue is both truly interdisciplinary and international in nature, which are necessary ingredients for a systematic analysis of these problems. The eight articles are authored by individuals from four different continents. Several of the articles are summarized below.

Godfrey Stadler identifies the status of data protection laws in his article. At the time he prepared his report, eight countries had enacted privacy or data protection legislation: Austria, Canada, Denmark, France, Norway, Sweden, the United States and West Germany. The Council of Europe had begun to draft a convention. Since Mr. Stadler's report two additional nations, Luxembourg and New Zealand, have enacted laws and many others are considering such legislation. In another article, Professor Herbert Maisl provides insight into France's law and the legal aspects of data flows between public agencies in his own country.

Stadler initially identifies the scope of applicability of each of the laws. They are distinguished on the basis of whether both public and private sector data bases are covered, whether automated and manual record keeping systems are encompassed and, very importantly, whether the definition of personal data covers legal persons as well as natural persons. This is the most controversial of the issues; whether data about corporations and other businesses should be regulated as well as information about individuals. In addition, Stadler describes the conditions for the release of informa-

tion to third persons in each law, the enforcement mechanisms and the controls imposed on personal data before it may leave the country.

He identifies seven basic principles which are incorporated in many of the laws. The first five are those which appear the most often:

> (1) the existence of an automated record system and the record keeper should be made public;
>
> (2) an individual should have a means of determining whether a record system contains information about him;
>
> (3) an individual should have the right to see information in a record system about himself;
>
> (4) an individual should have a means of correcting inaccurate, outdated or irrelevant information concerning himself;
>
> (5) special measures beyond traditional computer security precautions should be taken to protect personal information against accidental or deliberate access, alteration or dissemination;
>
> (6) information about individuals should be collected in a lawful and fair manner; and
>
> (7) information about racial origin, philosophical, political or religious views may not be collected unless the individual consents or a statute specifically allows it.

The European approach has been to pass omnibus laws rather than to target specific industries. Except for the United States and Canadian Acts, the laws apply to both the public and private sectors. Over half encompass manual as well as automated recordkeeping systems. Less than half apply to information about legal as well as natural persons but the trend appears to be to include legal persons. The enforcement mechanisms vary greatly. Only the United States Privacy Act of 1974 does not establish a data protection agency, but relies on the data subject to enforce legal rights by civil suit. Most of the countries regulate the flow of data across their borders; some provide for cooperation with foreign data protection authorities. The United States and Canadian laws alone exclude foreign data subjects from the scope of their protection.

The draft Convention on Data Protection of the Council of Europe is the subject of Heribert Golsong's article. The basic principles embodied in the document are that there shall be a free flow of information among the contracting states and the privacy of the subjects of such information shall be protected. Its provisions would, among other mandates, designate the applicable law in cases of transborder data flow and specify that all remaining conflicts between laws be resolved in favor of the data subject. Because such a convention requires a great deal of mutual agreement among the

contracting states, the Council of Europe, as a group of nations with common interests, is perhaps the best level at which to begin international cooperation in data protection, according to the author.

The convention may be ready for ratification by member countries by the end of 1980. Although the Carter Administration in the United States has been tardy in articulating the specifics of its policy of an unrestricted international flow of information while protecting individual privacy, State Department representatives have apparently been effective in persuading the Organization for Economic Cooperation and Development (OECD) to adopt this principle and that of limiting the applicability of such protection to natural persons as part of the OECD voluntary guidelines concerning transborder data flows. These voluntary guidelines, which cover only automated data bases, are apparently influencing the contents of, and speed with which agreement is being reached on the draft convention of the Council of Europe. Although the voluntary guidelines do not encompass legal persons, the trend of legislation is to cover both legal and natural persons. Thus, the outcome is still uncertain in Europe.

Justice M. D. Kirby of the Australian Law Reform Commission provides his views on the relationship of data protection and law reform. He concludes that no modern legal system can adequately deal with data protection by further development of existing legal principles. Justice Kirby believes there is a general consenus between nations as to the basic data protection to apply in legislation, but there is a great diversity in the manner in which they are to be enforced. He urges that countries now adopting data protection, or privacy protection laws participate in the work of international organizations in order to ensure the necessary harmonization and free flow of information.

Professor Wilhelm Steinmuller surveys the operational implications of legal problems for computer networks on the basis of their future social consequences. Since computer networks combine diverse social purposes with very different information technologies, various levels of social problems exist including "normal" automation problems such as disemployment and disqualification, additional informational type problems such as privacy, and special computer network problems such as transborder data flows and the "information sovereignty" of nations. He believes the only "new" problem may be the transborder data flow issue. Professor Steinmuller concludes that none of the legal problems of computer networks seem to be unsolvable if interdisciplinary work forces are applied to them.

Peter Rooms and John Dexter point out the overall operational

implications of data protection laws for private multinational communication networks. The emergence of such laws, according to the authors, will place additional constraints on computer network managers, system designers and operations personnel. Laws regulating transborder data flows could lead to major reassessments of processing strategies. However, the authors believe that traditional methods of network optimization using computer programs may be capable of modification to determine compliance requirements.

To maintain security, communications will have to be protected based on a cost-benefit analysis. Bulk encryption, random data flow and super-encryption may be required, according to Rooms and Dexter, but electromagnetic radiation and induction should be avoided. Security management measures should be formalized, and an overall balanced approach to maintaining privacy and security has the best chance of success, according to the authors.

COMPUTER NETWORKS is published by North-Holland Publishing Company, P.O. Box 211, 1000 AE Amsterdam, The Netherlands; 52 Vanderbilt Avenue, New York, New York 10017 (United States and Canada).

Fred M. Greguras