
An analysis of the cultural motivations for transborder data flow legislation

Transborder
data flow
legislation

37

Rita M. Walczuch

*Institut für Internationales Management der Karl Franzens Universität,
Graz, Austria*

Sanjay K. Singh

School of Business, University of Alabama at Birmingham, USA and

Todd S. Palmer

School of Business, Pennsylvania State University at Erie, USA

Introduction

The emergence of global information systems (GIS) has proven to be a catalyst for changes in the way one manages the multinational enterprise (MNE). Prior to the widespread use of GIS, the MNE mostly acted as an allocator of resources to its worldwide subsidiaries with each retaining a high degree of independence, given the information dispersion limitations (Miller, 1986; Mowlana, 1986). GIS has given the modern MNE options denied its earlier incarnations, primarily, to determine the degree of “connectiveness” it wishes to pursue in its global business strategy (Masmoudi, 1984; Roche, 1992). However, while the technology and systems infrastructure have advanced to give the MNE unparalleled possibilities to exploit synergistically business functions and units, there has also been the corresponding growth of significant man-made barriers to information dissemination (Jarvenpaa and Ives, 1993). These barriers, which are often in the form of transborder data flow legislation (TDFL), have the potential to limit data flows severely across national boundaries (Ajami, 1990; Boehmer and Palmer, 1993).

Pressure to enact TDFL may very well be expected to increase given recent movements by the European Union (EU). In October of 1992, the European Commission published a proposed directive which would require all of its member states to enact data protection legislation and bar the export of such data to non-EU states, unless the non member nation has an “adequate level” of privacy protection (Boehmer and Palmer, 1993). Certain national entities such as Hong Kong have already taken tentative steps to enact conforming legislation (Cooke, 1992; Jordan, 1994; Yue, 1992). Similar legislative initiatives from nations around the globe may be expected.

While some countries cite economic reasons for their legislation of TDF, the main driving force has been the concern for the privacy of the citizens (Guynes, *et al.*, 1990). The issue of privacy is essentially dependent on the cultural tenets

of a society (Buchholz, 1992). Past research to address this issue has been mostly anecdotal in nature (e.g. Ajami, 1990; Bennett, 1992). As such, we propose an examination of the cultural determinants of public policy. This will enable the IS managers at MNEs to analyse which nations are more likely to enact such legislation. With this knowledge, the MNEs may be able to influence the public policy formulation process to gain more favourable terms and, IS managers would be able to design and implement systems which could best deal with the cultural dimensions of TDF. In addition, the findings of the study will provide academics with a conceptual lens to analyse further the interaction of information technology and culture.

In this article, we first define TDF and present the status of TDFL. In addition, we discuss the implications of TDFL on IS managers. Then we develop a framework for examining the determinants of TDFL and investigate the relationship between culture and privacy protection. Thereafter, an exploratory analysis of TDFLs is conducted in context of Hofstede's (1980; 1991) findings on culture. The article concludes by emphasizing the need for continued research in this area.

Transborder data flow

Definition

TDF has been defined as the movement of data across national boundaries (Guynes *et al.*, 1990). Others have further qualified the definition to look at TDF in terms of the exchange of computer readable data across national boundaries using electronic means (Waples and Norris, 1992). Data can be operational, financial, personally identifiable, and scientific/technical in nature (Novotny, 1980). Not all types of data are subject to the same standard of legislation. However, it should be noted that the category of data that has catalysed the legislation of TDF is personally identifiable data or name linked data.

Need for TDFL

Rapid advances in telematics, coupled with the decreasing cost of computing, has drastically altered the assimilation, processing, and dissemination of information (Lee, 1994). Computers have replaced paper (and other similar media) as the conduit of information flow. Increasingly, individuals, organizations, and government are becoming critically dependent on telematics to transact business (Culnan, 1993).

Data are being collected across the globe on almost all aspects of life. These, in turn, are being used for decision making by various parties. Digital transaction on the information infobahn is omnipresent:

- electronic data interchange;
- electronic fund transfer;
- telebanking,
- telemedicine;

- teleshopping;
- interactive TV; and
- electronic commerce.

This has allowed virtually any involved entity to build electronic profile of consumers and potential clients (for example MarketPlace, a software/database about the purchasing behaviour of 120 million individuals in USA). The data can then be manipulated and matched with an endless number of databases, to extract information and project profiles that could not be even imagined a decade ago. As a result, “decisions having major impacts on individuals (such as whether or not to grant a loan, offer a sensitive job, or accept a life insurance proposal) are all too often made on the basis of these electronic profiles, almost regardless of their accuracy and without the knowledge of the individual(s) concerned” (Lee, 1994, p. 3).

While the computerization of a society has resulted in immense benefit to individuals, the potential threat to the privacy and wellbeing (economic and physical) of individuals have also increased. The inherent abuse is even greater when sensitive information is transmitted across national boundaries to foreign entities that are not regulated by the rules of the concerned nation(s). The latent problem of the electronic age has prompted governments to make the purveyors of public data more accountable and responsible for the collection and distribution of name linked information (Culnan, 1993). As a result, software/databases like MarketPlace are being withdrawn, credit reporting agencies are being denied licences in Europe, and nations with lax privacy laws are being threatened with economic sanctions by their trading partners.

Thus, the “respect for information privacy demands the enactment of data protection legislation which enshrines the information privacy right in working terms and covers both the public and private sectors” (Lee, 1994, p. 3). TDFL is a reality of international trade with which organizations and governments have to live with.

Current state of TDFL

The growth of TDF has increased the potential for conflict between the needs of individual privacy and business' requirements for the free flow of economic data and this has been of special concern to academics, business people, and policy makers (Ajami, 1990; OECD, 1980; Turn, 1979). This unsettling dichotomy has been of particular interest to European nations which have enacted a number of stringent privacy or data protection laws (Boehmer and Palmer, 1993; UNCTC, 1981). However, what is private and what is legal for TDF differs from country to country. France for example, protects personal data related to race, politics, philosophy, religion, union membership, and criminal record. In addition, no governmental or private decision can be based on the outcome of computer processing of data related to the personal profiles of individuals (Oz, 1994).

In Germany, there are strong feelings against the national census. Abuses committed by Nazis, based on extensive information on individuals, is fresh in the mind of the general population. Hence, the citizens are wary of sharing their private lives with their own government. As a matter of fact, every private organization employing five people and using computerized data processing is required to maintain a data controller, and in no case can organizations pass employee information without their consent (Oz, 1994). In general, European countries are much more sensitive to demographic related information than the USA. As a result, European data protection laws apply to all persons, whether public or private, corporate or real, involved in the usage and disclosure of name linked data (Lee, 1994). On the other hand, in the USA, the federal laws only cover public sector, with the state legislatures having the authority to regulate the private sector (Boehmer and Palmer, 1993).

Except for the very earliest of these laws, two documents have served as the framework for this expansive legislation:

- (1) the Organization for Economic Co-operation and Development's (OECD's) Guidelines; and
- (2) the Council of Europe's (CoE) Convention.

More recently, the European Commission (EC)'s 1992 Proposed Directive will have significant influence when approved by member states. A comprehensive description of these documents is beyond the scope of this article. For further elaboration on these agreements see Boehmer and Palmer (1993) and Oz (1994).

Motivations for TDFL

Two primary motivations for legislating restrictions on the flow of data across national boundaries have been the concern for the privacy and the economic wellbeing of a nation (Bennett, 1992). First, there has been the perceived need to protect the privacy of the citizen. Westin (1967, p. 7) defines privacy as, "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".

This was deemed especially important in the rationale of the early adopters of TDFL which based their legislation on the principle that technical applications should meet socially desirable ends and should not be driven exclusively by economic motives. In particular, data protection legislations were to ensure that the power inherent in holding information about people was not misused (Jay, 1991).

Furthermore, there was the fear in these states that foreign storage and dissemination could be used to circumvent national privacy laws (Chandran *et al.*, 1987; Mowlana, 1986). The issue of privacy led to the related issue of national sovereignty (Ajami, 1990). The ability to control information about their citizens is seen as a right and prerogative of the national government (Wigand, 1985). Many nation-states want to promote the wellbeing of its constituents by resisting what they see as the electronic colonization of their nation (Eger, 1979).

Several countries are not only concerned about the privacy of their citizen within their own country, but also try to ensure their citizens' right to privacy outside national boundaries. The concept of equivalent protection implies that a country can prohibit the export of protected data to countries with non-existent or less stringent data protection laws (Boehmer and Palmer, 1993). The CoE has called all signatories of its 1981 convention to enact legislation which would prohibit such transfer unless there is equivalent protection. This fact is followed by the 1992 EC Proposed Directive, although it applies a less rigorous standard of equivalent protection.

The economic motivations for TDFL are twofold:

- (1) Many countries want to protect their information technology industry by mandating that foreign corporations use local vendors for information processing requirements (Ajami, 1990).
- (2) Many countries have passed or proposed data protection legislation in order to continue free trading with countries that have enforced the concept of equivalent protection (Roche, 1992).

For these countries the potential economic loss in not being able to gain access to another nation's data is often seen to outweigh the loss over reduced control of their own data (Samiee, 1984).

Fifteen nations, primarily European, have adopted and nine countries have proposed TDFL (Cooke, 1992; Jay, 1991). Sweden was the first country to pass TDFL, restricting the flow of information between nations out of a concern for maintaining the privacy of their citizens when these data were transmitted to a nation without similar protection (Swedish Data Protection Act of 1973). Other countries (e.g. Austria, Canada, Denmark, France, Germany, Israel, Luxembourg, and Norway) soon followed with their own legislation in the late 1970s and 1980s for similar reasons of privacy protection.

However, after this point the motivations for the adoption of data protection legislation were mixed. While some countries proposed or passed laws out of a genuine concern for the privacy of their citizens, other countries proposed or implemented data protection legislation to be able to continue free trading with countries that have been enforcing the concept of equivalent protection. For example, Hungary was the first country from the Eastern bloc to consider TDFL and has made it very clear that it feels a need to adopt conforming legislation because it fears it will be excluded from trade with the EU (BBC, 1992a; 1992b).

In North America, data protection laws in the USA have their roots in the concern for the privacy of US citizens. However, there is also concern that the EC will prohibit their members from exporting personal data to countries with inadequate data protection laws, among others, the United States (Amidon, 1992). Canada is in the process of revising its data protection legislation so that European standards will be met (Perrin, 1992; McKenzie, 1992). Among the Asian countries Hong Kong is also considering data protection legislation for similar reasons (Cooke, 1992; Jordan, 1994; Yue, 1992).

While clearly both privacy and economic concerns are important drivers in the growth of TDFL, this study will focus on the privacy aspect for four reasons:

- (1) The 1992 EC Proposed Directive is an instrument which, though it purports to balance privacy and economic issues, clearly leans towards the protection of personal privacy (Boehmer and Palmer, 1993). In addition the CoE Convention also emphasizes privacy as the prime determinant of TDFL. These two documents reflect the values of the European nations, where the concern for privacy of citizens outweighs the economic consequences of restricting TDF. Given that the EC is the major player in TDFL, an extended examination of this issue is warranted.
- (2) For the NICs and LDCs, who are the other major players in the controversies regarding TDF, the concern is one of privacy. While the countries understand the economic benefits from a freer flow of information, and some countries want to become the "data havens" of the future, the concern for privacy precludes them from eradicating the electronic boundaries of the nation (Miller, 1986; Oz, 1994). The political powers realize that access to certain types of information have the capability to give other nations a competitive advantage, and may jeopardize the security and the privacy of the individuals. Thus, these countries prohibit foreign access to information like R&D data, financial, economic, political, cultural, and any other type of information that may be compromising (Oz, 1994).
- (3) Most managers of MNEs are familiar with national economic parameters which constrain organizational decision making. They are much less knowledgeable about the impact of cultural artefacts, such as privacy considerations, in assessing an organization's environment. Given this paucity of understanding, an analysis of the public policy formulation regarding privacy protection is necessary before examining the economic dimensions of the issue.
- (4) Many economic conflicts can be and have been resolved through mutual agreements sponsored by UN or other international bodies, but privacy laws rooted in cultural differences are still not in harmony (Oz, 1994).

TDFL – implications for IS managers

The expanding kaleidoscope of national legislation related to TDF presents a significant challenge to the information system professional. For technical and systems requirements will not only be of importance, but also the changing political landscape of the global community. This problem is not restricted only to countries with existing national legislation to which the MNE can despatch its contingent of highly trained attorneys. After the fact, perhaps the greater problem and correspondingly greater opportunity lies with those nations which

currently have no TDFL but may enact it. The enactment of these statutes has promoted concerns relating to the following.

Lack of uniformity in TDFL

These statutes have not been uniform in either content or process, despite the existence of several international conventions (Woody and Fleck, 1991). Since most of these laws mandate that transfers to other nations will only take place if these countries have “equivalent protection”, the IS manager must be aware of the laws of all nations in which the data were either collected, stored, or disseminated (Reidenberg, 1992).

Increased statutory duties

In order to operate data facilities located in Europe, the IS manager must comply with significant duties in all aspects of data processing. As contemplated by the 1992 EC Proposed Directive some of these duties would include the following:

- all data collected must meet stated quality standards;
- advance notice must be given in most situations;
- data subjects must be notified when the outcome of computerized processing is used against them;
- data subjects must be notified in certain cases when data is transferred to third parties;
- data subjects must be granted access to data; and
- data must be prohibited from being processed if it fails to satisfy a series of preconditions.

Increased liability for IS managers

The 1992 EC Proposed Directive would place direct personal liability on the “controller of the data”. A reading of the comments of the document indicates that the “controller” is intended to be a person and not the business entity. In most instances, this person will be the IS manager. This liability looms only larger when one considers that the controller will have increased statutory duties and that persons who are harmed will be able to obtain judicial and “dissuasive penalties”. The Proposed Directive is silent as to whether liability is to be joint and several or whether indemnification of the controller is permitted. Given this increased liability, one may assume that this may lead to a “chilling effect” on IS managers as they go about designing and implementing systems (Bohmer and Palmer, 1993).

Decline in outsourcing

This increased liability may also factor into a firm’s decision on whether to outsource data processing functions. A reading of the 1992 EC Proposed Directive implies that the data controller will be ultimately liable for compliance

ITP
8,2

with all aspects of the directive. Given the inherent lessening of control involved in an outsourcing situation, this may well lead to firms avoiding outsourcing.

Duplication of IS facilities

44

Xerox was forced to open a duplicate data processing system in Sweden, even though its London based IS facility was capable of handling all European related data. The reason? The Swedish TDFL mandates that all processing of information relating to Swedish citizens be conducted in Sweden (*Data Processing*, 1986).

Data transfers prohibitions

Under most countries' current statutes, if the country which the data are being transferred to lacks equivalent privacy protection, then the transfer may be barred. Recently, a German bank refused its Hong Kong branch's request for access to customer information concerning German citizens in fear that this transfer would violate the Bundesdatenschutzgesetz, i.e. Federal Data Protection Act, (Choy and Boyd, 1992). Sony Germany's request to export German consumer information to the United States was denied (Ratcliffe and Waltz, 1992). In 1991 the French Data commission prevented the Italian automobile maker, Fiat, from electronically transferring personal records between France and Italy (Rothfeder, 1992).

Currently, individual European nation's statutes offer a *smorgasbord* of duties with even the common ones between nations having their own unique nuances. The plethora of statutes means that IS managers must spend an increasingly large amount of time assuring that their firm's data processing facilities comply with local ordinances.

However, the 1992 EC Proposed Directive, as presently written may promote the creation of data havens. Despite the apparent complexity and thoroughness of the written proposal, it permits individual EU members considerable leeway in enacting their own national legislation. The basic overriding principle of the proposal is that once the name-linked data meet the requirements of the TDFL of any individual member, they are free to flow through the entire community. Nations such as Spain, Italy, and Greece, which have virtually no tradition of data protection, may enact more liberal legislation. The result of this may be that data collected in a particular manner that is barred under one of the member states' current statutes may be permitted under the laxer legislation of another nation (Boehmer and Palmer, 1993).

TDFL – a conceptual framework

The concept of privacy protection through public policy formulation is in essence an issue of the values and ideologies that are held to be important by individuals and that are institutionalized in any individual culture (Ajami, 1990). From this perspective, the legitimization of these values and ideologies through the public policies is aimed at reflecting the beliefs of individuals and to protecting the integrity of the citizens (Bennett, 1992).

Values, is a term which has an objective and subjective component. Buchholz (1992, p. 118) comments, “values are different between people and reflect individual desires and beliefs. Values are properties that human beings associate with or assign to certain forms of human behavior, institutions, or material goods and services”.

From this subjective viewpoint, values are not an intrinsic element of the object or behaviour in question; rather, the decision defining a particular value is derived through individuals making personal judgements. This is in contrast to an objective perspective where values are derived outside the personal experiences of those individuals faced with choices. In this situation values are part and parcel of the behaviour or object in question.

Despite this framework, it should be noted that there is no clear rationale, either objective or subjective, which presides over the defining of values. Rather there is a complex interaction between these two perspectives which leads to the creation of societal values, which are commonly held values that are believed to produce desirable outcomes for society as a whole (Buchholz, 1992; Daleiden, 1990). The conflict between the objective and subjective viewpoints is resolved through the essence of public policy formulation process, i.e. negotiation and compromise (Rule, 1974; Sieghart, 1984).

Ideology is the other term associated with the public policy formulation process. Ideology, according to Buchholz (1992, p. 124), “consists of a shared set of beliefs that are representative of a group of an entire society ... and is the framework of ideas that integrates and synthesizes all aspects of a group’s or society’s experience into a meaningful whole”.

Legislation serves to protect what individuals in a society may value (privacy for instance) and is the formal manifestation of a society’s ideology. Thus, privacy or any desired behaviour, may only be institutionalized when there is an ideological rationale for it. One such ideological rationale for privacy has been succinctly stated by Justice (1970, p. 4): “above all we need to be able to keep to ourselves, if we want to, those thoughts and feelings, beliefs and doubts, hopes, plans, fears and fantasies, which we call ‘private’ precisely because we wish to be able to choose freely with whom, and to what extent, we are willing to share them”.

While benefits, hopes and fantasies are not what people want to be precluded, it is the quantifiable, hard, name-linked demographic data that people and government want to be prevented from being transported across the boundaries of their own country. In any society where the debate concerns privacy, the ideology provides an instrument to bring societal activity into focus on this issue and serves to provide guidance to individuals on how it should respond to changes in values (Shils, 1979). Ideology provides a blueprint in making decisions (Feliks, 1985).

Therefore the two fundamental constructs of public policy formulation are the values and ideologies prevalent in a society. Buchholz (1992) presents a framework of public policy formulation which suggests that to understand the

determinants of such legislations, an examination of a society's values and ideologies is a necessity.

Hofstede (1984; 1991) looks at values and ideologies in terms of them being reflections of a society's culture. Hofstede (1991) provides a typology by which these broad constructs, values and ideologies, may be operationalized. By observing how Hofstede (1984; 1991) and Buchholz (1992) look at values and ideology, we can describe a framework which links culture and the public policy formulation process (see Figure 1). With an assumption that values and ideologies serve as the basis for public policy formulation, we argue that an examination of how public policy is formed necessitates an appraisal of the society's culture. Furthermore, by studying certain aspects of a society's culture, a model of the creation of the outputs of public policy formulation, specifically TDFL, may be constructed.

In the next two sections we will examine various definitions and dimensions of culture and analyse TDFL in light of the different attributes of culture.

Culture

Definition and attributes

The construct of "culture" has been given a multitude of definitions. However, one of the most influential definition to date is of Hofstede's (1984, p. 21). Culture is seen as: "the collective programming of the mind which distinguishes the members of one group or society from those of another".

Hofstede (1984; 1991) expanded on his definition of culture by describing five empirically derived dimensions through which cultures may be distinguished from one another. These dimensions represent the common structure in the cultural systems of different societies, and serve as a guide in positioning nations in a cultural schema. The five dimensions are individualism, power distance, uncertainty avoidance, masculinity, and time orientation. The first four dimensions were catalogued as a result of Hofstede's 1980 study. Time orientation was added as the fifth dimension (Hofstede, 1991) after data from other research efforts found an unexplainable dimension among Asian countries. Hofstede (1980) used a total of 117,000 questionnaires, in 20 languages, from 88,000 respondents in 66 countries. The survey instrument

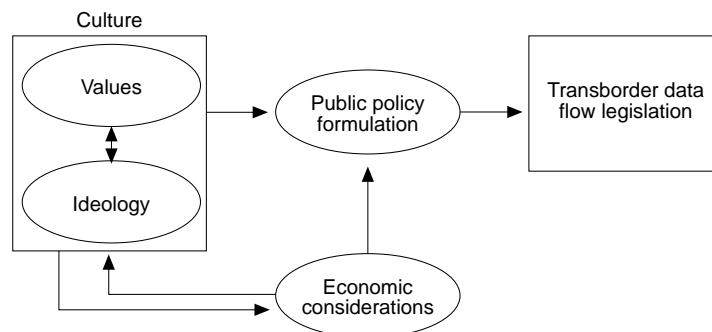


Figure 1.
Determinants of TDFL

included 160 questions, of which 63 were related to the construct of value. For the purposes of generalizability, all respondents were chosen from the same multinational corporation, IBM.

The individualism measure deals with the relationship between an individual and others. The majority of people in this world live in collectivist societies. In a collectivist society the interests of the group prevail over the interests of the individual. Most Asian, South American and African countries have collectivist cultures (e.g. Japan, Venezuela, and the West African countries). On the other hand, a minority of people live in individualistic societies, where the interests of the individual prevails over the group. Individualistic countries include most Western nations (e.g. France, Germany, Great Britain, Sweden, and the USA).

Power distance is a measure of the society's acceptance of an unequal distribution of power. A society which has a high power distance accepts an unequal distribution of power. On the other hand, if the society emphasizes equal rights for everyone, the power distance score is low. The power distance dimension and the individualism dimension are negatively correlated with each other, i.e. individualistic cultures tend to have a low power distance while collectivist cultures tend to have a high power distance score. However, Hofstede (1984) argues that power distance and individualism are still two different constructs and should be treated as such. For example, France, Belgium, and Italy have an individualistic culture but a high power distance.

The third measure, uncertainty avoidance, measures the degree to which members of a society try to avoid uncertainty by planning or by other means. A low uncertainty avoidance score means that the culture is not worried about an uncertain future. Examples of such countries with low uncertainty avoidance are most South American countries, the Scandinavian countries (except for Finland), Canada, and Great Britain. On the other hand, societies with high uncertainty avoidance try to regulate all possible behaviour with rules and laws to be able to control or at least predict the future. Examples of cultures with high uncertainty avoidance include most southern European countries, Israel and all German speaking countries.

The masculinity index is a measure of the kinds of value that are predominant in a society. Typically, values such as showing off, power, and personal achievement dominate in a masculine society (e.g. Japan, most northern European, North American countries). Feminine societies value team spirit, modesty, and helping others. Examples of feminine cultures include most South American and Asian countries.

The fifth and last dimension, time orientation, refers to a long-term versus a short-term perspective in life. A society with a long-term orientation is more inclined towards the future while a society with a short-term orientation is more concerned about the present and past. Asian countries typically have a long-term orientation, while most Western cultures have a short-term orientation.

Hofstede's categorization does not necessarily mean that all individuals in a society will have a particular cultural orientation. Rather, the implication is that, under certain circumstances, an individual, for example in an Asian

society, will have a longer time orientation than his/her counterpart in a Western country.

Criticism of Hofstede's model

Research has shown that Hofstede's findings provide an excellent basis for cross-cultural evaluations. Various intercultural studies have been based on this framework and numerous studies have been able to confirm his results (Gudykunst and Ting-Toomey, 1988; Shackleton and Ali, 1992). As Jordon (1994, p. 5) states, "its authority is enhanced by its predictive ability and its synthesis of partial results". However, Hofstede's (1980) model is not without shortcomings. Any interpretation of Hofstede's model should be made in light of the following limitations pointed out by Jordon (1994) and Berry *et al.*, (1992):

- The four quadrants in the scatter diagram of uncertainty avoidance against power distance (see Figure 2) were based on an arbitrary division, and not on the values of the mean or the median. Hofstede's aim was to put his country, The Netherlands, as the nearest to the norm. However, if one recalculates the data using bivariate mean or median, the country nearest to the norm would be Pakistan.
- The categorization of the nations were not made using statistical techniques like cluster analysis. Rather, Hofstede used ethnicity and culture as the basis for grouping the nations. By analysing all the four original dimensions, the nation that emerges as the model is Iran. This is quite contrary to the events that have taken place in that country in the last two decades. In addition, Hofstede grouped many countries into a region without regard to the vast differences in language, customs, and other cultural attributes.
- The definition of the five dimensions were more broader than could be justified by the number of items used to measure the constructs, in particular power distance and uncertainty avoidance.
- Hofstede's study had some methodological problems. First, data were collected from only one segment of the society, i.e. the middle class and that too, from a single company. This results in non-generalizability of the finding to the population at large. Second, while statistical difference between individual countries was significant (50 per cent), the amount of variation among individuals was quite low (4.7 per cent). Many of the statistically significant findings may have been due to the large sample size. Third, Hofstede's dimension were constructed on a group level. However, his conceptualization the construct value was on an individual level, as was the collection of data.

Other researchers have identified additional dimensions of culture (e.g. Hall, 1976; Hall and Hall, 1990). However, they do not offer any qualitative measures or scopes for their dimensions and can thus not be used in our study. Hofstede's

(1980; 1991), framework is still the most comprehensive, empirically derived classification scheme for national cultures available to date.

TDFL – analysis of cultural motivations

In this section we analyse possible cultural explanations for the adoption of TDFL. Although there are differences between the data protection laws passed in the various countries we focus on the similarities between the cultures of countries that adopted data protection legislation versus the countries that have not. These similarities are also used to explain why some of the countries that have proposed data protection legislation have not succeeded in meeting EU requirements for TDFL.

Table I shows Hofstede's five dimensions for all countries that adopted or proposed data protection legislation so far. To facilitate our analysis, the value for the dimensions is either high (above neutral) or low (below neutral). The neutral point is the value that would result if each item for the dimension was answered as neither agree nor disagree. On further elaboration on the calculation of the value for each dimension please see Hofstede (1984; 1991). We would like to caution the reader that the sample size is too small and the statistical methods too rudimentary to make broad, generalizable conclusions. Our finding merely identifies a pattern, and provides a conceptual framework for further empirical analyses of the hypothesized relationships.

The countries are listed in chronological order according to the year that data protection legislation was first adopted. Each country is assigned to one of three groups: early adopters (1973-1981), late adopters (1982-1992), or countries that have proposed legislation. The year 1981 was chosen as cut-off point because that year the CoE ratified the first international data protection agreement that required its members to enact conforming legislation.

Out of 24 nations, data are available on 21 nations for the first four dimensions of culture. For time orientation, data is available only on eight nations. The number of low and high threshold values for each of the attributes is given in Table II. An analysis of the frequency counts shows that two dimensions of culture seem to be correlated with the adoption of data protection legislation: power distance and individualism. Not enough data are available for the time orientation dimension, but it seems as if the time orientation score is negatively related to the adoption of data protection legislation. Neither the uncertainty avoidance nor the masculinity/femininity measure seem to be correlated with the adoption of data protection legislation.

Most countries that have adopted data protection legislation so far have a power distance measure that is below the threshold value in Hofstede's (1980; 1991) study. This suggests that cultures that do not accept an unequal distribution of power (i.e. the culture feels that everyone should have the same rights and privileges) are more inclined to enact data protection legislation. In the context of the purpose of TDF it makes sense as these legislations are aimed at protecting individuals from the exploitation of MNEs or other nation-states.

Countries	Uncertainty avoidance	Power distance	Individualism	Masculinity	Time orientation
<i>Early adopters (1973-1981)</i>					
Sweden (1973)	L	L	H	L	L
Germany (1977)	H	H	H	H	L
Austria (1978)	H	L	H	H	-
Denmark (1978)	L	L	H	L	-
France (1978)	H	H	H	L	-
Norway (1978)	L	L	H	L	-
Luxembourg (1979)	-	-	-	-	-
Israel (1981)	H	L	H	L	-
<i>Late adopters (1983-1992)</i>					
Canada (1982)	L	L	H	H	L
UK (1984)	L	L	H	H	L
Iceland (1985)	-	-	-	-	-
Finland (1987)	H	L	H	L	-
Iceland (1988)	L	L	H	H	-
The Netherlands (1988)	L	L	H	L	L
Australia (1989)	L	L	H	H	L
<i>Proposed legislation</i>					
Belgium	H	H	H	H	-
Greece	H	H	L	H	-
Italy	H	H	H	H	-
Hong Kong	L	H	L	H	H
Hungary	-	-	-	-	-
Portugal	H	H	L	L	-
Spain	H	H	H	L	-
Switzerland	H	L	H	H	-
USA	L	L	H	H	L
<i>Notes:</i>					
L = below the threshold					
H = above the threshold					
- = no information available					
<i>Source:</i> Hofstede (1991)					

Table I.
Cultural attributes of nations that have passed or proposed transborder data flow legislations

All adopters of data legislation have a high individualism measure. This suggests that cultures that put a higher value on individuals' interests are more likely to adopt data protection legislation. Intuitively this makes sense since the main purpose of data protection legislation is to protect the individuals' rights.

The values for the power distance of members of the European Community that have not yet adopted data protection legislation (Belgium, Greece, Italy, Portugal, and Spain) are all high. This may explain why these countries were not yet able to agree on specific data protection legislation. For example, after

Attributes	TDFL	Low	High
Uncertainty avoidance	Adopted	8	5
	Proposed	2	6
Power distance	Adopted	12	1
	Proposed	2	6
Individualism	Adopted	0	12
	Proposed	3	5
Masculinity	Adopted	7	6
	Proposed	2	6
Time orientation	Adopted	6	0
	Proposed	1	1

Transborder
data flow
legislation

51

Table II.
Frequency counts of
cultural attributes

six years of discussion the Spanish government sent a data protection bill to parliament, but it did not meet European standards (Business International, 1991). Many exceptions for several administrative units made the bill almost useless. In addition, the government reserved the right to have full hiring and firing control over the director of the enforcement agency which decreased the power of the enforcement agency drastically.

The high value for the power distance may be used to explain this development. The various government agencies simply did not want to give up any of their rights and privileges, and the culture of the country did not object to the unequal distribution of power. In addition, Greece and Portugal are collectivist societies, contrary to the attributes of nations that have adopted TDFL. Therefore, these two countries will have the most difficulty in enacting TDFL.

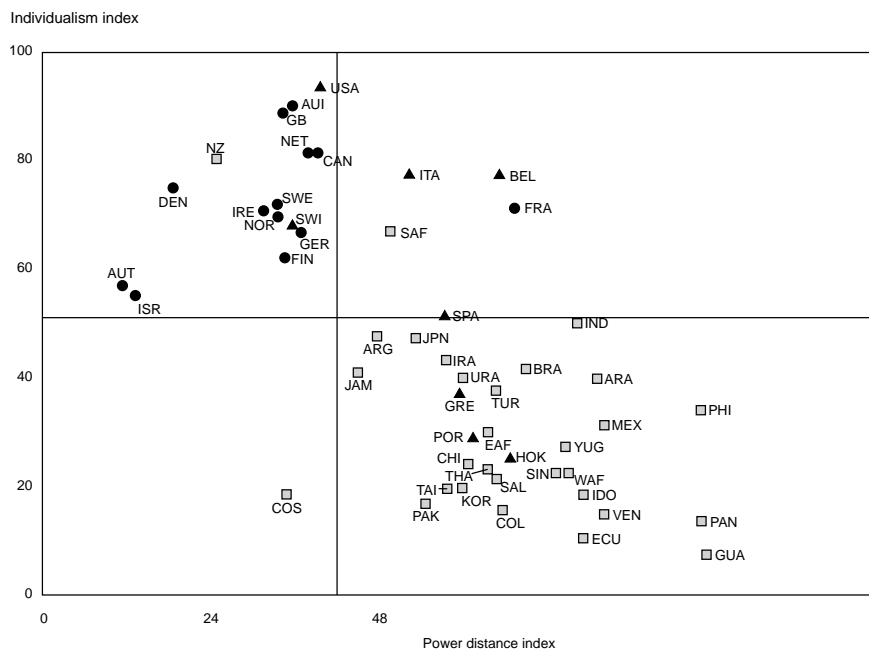
The low power distance values for the USA and Switzerland supports the conjecture that those two countries have proposed privacy legislation out of concern for their citizens' privacy. Further, these two nations have high individualism scores which corresponds with the scores of the adopters. Therefore, it can be expected that legislation regarding TDF will be enacted with relative ease in the USA and Switzerland. Hong Kong's high power distance and low individualism scores on the other hand supports the notion that Hong Kong is interested in passing data protection legislation to avoid EU restrictions. The same can be argued for Belgium, Greece, Italy, Portugal, and Spain to pass TDFL.

As a next step the power distance and individualism scores of countries that have neither adopted nor proposed data privacy laws were compared with those countries that have. Hofstede (1991, p. 54) compiled a two-dimensional graph of all 50 countries and three regions in his study (see Figure 2). The graph classifies all 53 countries or regions into one of four quadrants: low power distance/low individualism, low power distance/high individualism, high power distance/high individualism, and high power distance/low individualism. We amended the graph slightly to classify countries that have adopted/proposed

data protection legislation or have not adopted/proposed TDFL. As can be easily seen from Figure 2, France is the only country outside the low power distance/high individualism quadrant that has adopted data protection legislation.

New Zealand is the only country in the low power distance/high individualism quadrant that has not adopted or proposed data protection legislation. However, the dimensions of culture suggests that data protection legislation is an issue for New Zealanders. One explanation for their lack of TDFL might be the relative agrarian economy of New Zealand.

Only six countries (besides France) in the other three quadrants have proposed data protection legislation – Belgium, Greece, Hong Kong, Italy, Portugal and Spain.



Key:

- ▲ Adopted legislation
- Proposed legislation
- No legislation

ARA	Arabic speaking countries (Egypt, Iraq, Kuwait, Lebanon, Libya, Saudi Arabia, United Arab Emirates)	EQA	Ecuador	JAM	Jamaica	SAL	El Salvador
ARG	Argentina	FIN	Finland	JPN	Japan	SIN	Singapore
AUI	Australia	FRA	France	KOR	Korea	SPA	Spain
AUT	Austria	GB	Great Britain	MAL	Malaysia	SWE	Sweden
BEL	Belgium	GER	Germany	MEX	Mexico	SWI	Switzerland
BRA	Brazil	GRE	Greece	NET	The Netherlands	TAI	Taiwan
CAN	Canada	GUA	Guatemala	NOR	Norway	THA	Thailand
CHI	China	HOK	Hong Kong	NZL	New Zealand	TUR	Turkey
COL	Colombia	IND	India	PAK	Pakistan	URU	Uruguay
COS	Costa Rica	IDO	Indonesia	PAN	Panama	USA	USA
DEN	Denmark	IRA	Iran	PER	Peru	VEN	Venezuela
EAF	East Africa (Ethiopia, Kenya, Tanzania, Zambia)	IRE	Ireland	PHI	Philippines	WAF	West Africa (Ghana, Nigeria, Sierra Leone)
		ISR	Israel	POR	Portugal	YUG	Yugoslavia
		ITA	Italy	SAF	South Africa		

Source: Hofstede (1991, p. 54)

Figure 2.
Hofstede's 53 countries and regions:
Individualism vs.
Power Distance indices

Portugal, and Spain. As we argued earlier, these countries may have considered data protection legislation to avoid trade sanctions from EU members. Figure 2 also suggest that many South American, Middle Eastern, African and Asian countries will not adopt TDFL voluntarily. This includes Japan, one of the major economic powers in the world. It can be expected that Japan, like Hong Kong, will propose to adopt data protection legislation to avoid the restrictions the EU is posing on countries with inadequate protection.

All the NICs and LDCs have attributes that are the exact opposites, i.e. high power distance and low individualism. When these nation-states propose/adopt TDFL it will be for reasons other than a concern for the privacy of its citizens. As Ajami (1990, p. 131) notes, most of these nations are interested in: "a more equitable share on a global basis, the increasing economic gains which are resulting from the telecommunication revolutions".

However, there may be political and technical reasons for not proposing/adopting TDFL. For example, the uses of computer technology in these countries (with the exception of Singapore) is not as pervasive as in Europe or the USA. Most of the data are still collected, maintained, and processed in article format. Thus the volume of computerized transaction is not sufficient to justify concerns for TDFL (Oz, 1994).

In addition, many nations have political reasons for not proposing/adopting TDFL (Boehmer and Palmer, 1993). These countries have a totalitarian approach towards maintaining/regulating name linked data. MNEs cannot access and transport information related to individuals. The nations feel vulnerable to being electronically exploited by more advanced nations in the areas of national security and cultural manipulations (Miller, 1986) and erect following types of barrier to the free flow of information (Ajami, 1990, p. 132):

- discriminatory pricing of data transmission services;
- mandated use of national data networks;
- denial of lease lines or restrictions on use;
- requiring processing of data in country of origin;
- restrictions on the importation of hardware and software; and
- customs duties and value-added taxes on information entering or leaving the country.

Thus, there is no need for TDFL. However, the bigger problem is that if and when the NICs and LDCs propose/adopt TDFL, the problem will not be in the enactment of the legislation but in its enforcement. Many of these countries are stretched to their limits trying to cope with the growth/expansion of their economies. They may not have the resources to expend on the enforcement of further legislation (Oz, 1994).

Conclusions

Recent advances in telematics has made TDF a reality. To a great extent, the technology and systems aspects of TDF have been resolved, but the legal and political dimensions remain. Nations around the world are becoming

increasingly knowledgeable about the various invasive aspects of TDF. As a result these countries are creating a multitude of statutes to protect what they see as important national interests. Calls for defending the economic base and the privacy of their people are becoming much more commonplace. This evolution has created correspondingly greater challenges for the IS manager. For no longer may this person be skilled solely in terms of technical and organizational abilities, but he/she must have a truly global outlook with a specific knowledge of many different national statutes.

Recent international political news indicates that the enactment of TDFL around the world will only increase. With the expected passage of the 1992 European Proposed Directive this trend should be heightened as nations, particularly those with a strong economic connections to the EU, adopt conforming legislation. However, these non-EU states' resulting legislation will be a hodgepodge of process and content, making it difficult for IS managers to comprehend the basics of these laws, much less the nuances. Complicating this scenario is that the possibility of some type of worldwide agreement pertaining to uniform TDFL is highly unlikely. If the recent confrontation at the GATT talks concerning TDF are any indication, a binding, comprehensive agreement is a long way off.

Given that IS managers must be able to anticipate and respond to a changing political environment, this exploratory study creates a framework for classifying TDFL. Utilizing Hofstede's (1980, 1991) five dimensions of culture, we found that the power distance and individualism dimensions appear to correlate with the adoption of TDFL. Nations with cultural attributes which emphasize an equal distribution of power and the dignity of the individual appear more likely to adopt TDFL out of privacy concerns. Nations with values in the opposite direction would appear less likely to enact TDFL. The adoption of such statutes in these countries would appear to be a response to the economic pressure to continue normal trading relations with those nations which have adopted TDFL. The reason may also be the increasing computerization of the society, making TDF an integral part of transacting business.

What does this study mean for IS managers? The article provides them with a conceptual lens to discern between nations that have adopted and proposed TDFL, and at the same time anticipate with a reasonable degree of accuracy which nations may enact TDFL. Nations which adopt TDFL out of strong concern for individual privacy, which is reflected in their power distribution and individualism scores, would probably have stricter TDFL than those with low scores. On the other hand, nations with high power distance and low individualism assessments which adopt TDFL for other reasons would probably have more lenient provisions. A key question as to any type of legislation is whether the nation has the means and will to enforce it. While those nations which have basically an economic motive and a low regard for privacy may enact TDFL, they may not have the determination to enforce such a law.

Such a framework may be of assistance to IS managers as they develop international IS strategy. For instance, an examination of Figure 2 indicates that of the nations proposing TDFL, four are nations with low individualism and

high power distance scores. All four primarily have economic motives in adopting such legislation; Spain, Greece, and Portugal in order to stay in step with the EU, and Hong Kong in anticipating monetary loss for its financial industry if it fails to enact "adequate protection" for data transfers. All four of these nations will probably enact TDFL in the future but with lenient provisions for its enforcement. This is vital information for IS and other senior level managers in the strategy formulation process.

Obviously, this study is only a first attempt at examining the impact of culture on the public policy formulation process involving TDFL. Future studies need to examine more thoroughly other aspects (e.g. economic, political, technical) of TDF. Further, in-depth content analysis of the laws of countries that have adopted/proposed TDFL is required. Also, researchers need to examine whether countries enacting TDFL for the protection of individual rights, are also concerned with protecting the intellectual property rights of firms. In general, there needs to be a greater awareness among IS researchers about the reciprocal relationship between culture, politics, economics, and the adoption and diffusion of technology across national boundaries.

References and further reading

- Adler, N.J., Doktor, R. and Redding, G.S. (1986), "From the atlantic to the pacific century", *Journal of Management*, Vol. 12 No. 2, pp. 295-318.
- Ajami, R. (1990), "Transborder data flow: global issues of concern, values, and options", in Lundstedt, S.V. (Ed.), *Telecommunications, Values, and the Public Interest*, Ablex Publishing Corporation, Norwood, NJ.
- Amidon, P. (1992), "Widening privacy concerns", *Online*, Vol. 16 No. 4, pp. 64-7.
- Barnouw, V. (1963), *Culture and Personality*, The Dorsey Press, Homewood, IL.
- Bennett, C.J. (1992), *Regulating Privacy*, Cornell University Press, Ithaca, NY.
- Berry, J.W., Poortinga, I.M., Segall, M.H. and Dansen, P.R. (1992), *Cross-cultural Psychology: Research and Applications*, Cambridge University Press, Cambridge, MA.
- Boehmer, R. and Palmer, T.S. (1993), "The 1992 EC data protection proposal: an examination of its implications for US business and US privacy laws", *American Business Law Journal*, Vol. 31 No. 2, pp. 265-31.
- British Broadcasting Corporation (BBC) (1992a), "Bill on personal data protection submitted to national assembly", *Summary of World Broadcasts*, 15 May.
- British Broadcasting Corporation (BBC) (1992b), "Telecommunications bill presented to parliament", *Summary of World Broadcast*, 10 October.
- Buchholz, R.A. (1992), *Business Environment and Public Policy: Implications for Management and Strategy*, Prentice-Hall, Englewood Cliffs, NJ.
- Business International (1990), "Switzerland strengthens law", *Business Europe*, 6 April.
- Business International (1991), "Data regulation: Spain's new law: late and lax", *Business Europe*, 12 July.
- Chandran, R., Phatak, A. and Sambharya, R. (1987), "Transborder data flow: implications for multinational corporations", *Business Horizons*, November-December, pp. 74-82.
- Choy, L. and Boyd, A. (1992), "Hong Kong: local bank caught in a crossfire of data protection battle", *South China Morning Post*, 30 November.
- Cooke, J. (1992), "Hong Kong: warning over data legislation", *South China Morning Post*, 28 October.

- Country Report* (1990), "Political development: EC membership question", *Economist Publications*, 8 May.
- Culnan, M.J. (1993), "How did they get my name: an exploratory investigation of consumer attitude toward secondary information use", *MIS Quarterly*, Vol. 17 No. 30, pp. 341-61.
- Daleiden, J.L. (1990), "Social considerations in the development of telecommunications policies", in Lundstedt, S.B. (Ed.), *Telecommunications, Values, and the Public Interest*, Ablex Publishing Corporation, Norwood, NJ.
- Data Communications*, (1986), "Transborder data flow: an old problem remains unsolved", Editorial, Vol. 13, April.
- Eger, J.M. (1979), "US proposals for progress through negotiations", *Journal of Communications*, Summer, pp. 124-30.
- Elbing, A.O. and Elbing, C.J. (1967), *The Value Issue of Business*, McGraw-Hill, New York, NY.
- Feliks, G. (1985), *Ideologies, Goals and Values*, Greenwood Press, Westport, CT.
- Gudykunst, W. and Ting-Toomey, S. (1988), "Culture and affective communication", *American Behavioural Scientist*, Vol. 31 No. 3, pp. 384-400.
- Guynes, J.L., Guynes, S.C. and Thorn, R.G. (1990), "Conquering international boundaries that restrict the flow of data", *Information Strategy: The Executive's Journal*, Vol. 6 No. 3, pp. 27-32.
- Hall, E.T. (1976), *Beyond Culture*, Doubleday, Garden City, NY.
- Hall, E.T. and Hall, M.R. (1990), *Understanding Cultural Differences*, Intercultural Press, Yarmouth, ME.
- Hofstede, G. (1980), *Culture's Consequences: International Differences in Work-related Values*, Sage Publications, Beverly Hills, CA.
- Hofstede, G. (1984), *Culture's Consequences: International Differences in Work-related Values*, Sage Publications, Beverly Hills, CA.
- Hofstede, G. (1991), *Culture and Organizations: Software of the Mind*, McGraw-Hill Book Company, London.
- Jarvenpaa, S.L. and Ives, B. (1993), "Organizing for global competition: the fit of information technology", *Decision Sciences*, Vol. 24 No. 3, pp. 547-80.
- Jay, R.P. (1991), "Transborder data flow", *New Law Journal*, Vol. 141 No. 6492, p. 241.
- Jordon, E. (1994), "National and organisational culture: their use in information systems design", Working Paper Series No. WP94/08, City Polytechnic of Hong Kong, Kowloon, Hong Kong.
- Justice (the British Section of the International Commission of Jurists) (1970), *Privacy and the Law*, Justice, London.
- Kroeber, A.L. and Kluckholm, C. (1952), *Culture – a Critical Review of Concept and Definitions*, Harvard University Press, Cambridge, MA.
- Lee, M. (1994), "Information privacy legislation: the case of Hong Kong", Working Paper Series No. WP94/03, City Polytechnic of Hong Kong, Kowloon, Hong Kong.
- McKenzie, R. (1992), "Canada waits for EC rules on personal data transfers: business fallout feared", *The Financial Post*, 23 March, p. 10.
- Masmoudi, M. (1984), "The new world information order and direct broadcasting satellites", *Syracuse Journal of International Law and Commerce*, Vol. 8 No. 322, pp. 322-42.
- Miller, A.P. (1986), "Teleinformatics, transborder data flow and the emerging struggle for information: an introduction to the arrival of the new information age", *Columbia Journal of Law and Social Problems*, Vol. 20 No. 89, pp. 89-114.
- Mowlana, H. (1986), *Global Information and World Communication, New Frontiers in International Relations*, Longman, New York, NY.
- Novotny, E.J. (1980), "Transborder data flow and international law: a framework for policy-oriented inquiry", *Stanford Journal of International Law*, Vol. 16 No. 141, pp. 431-9.
- Organization for Economic Co-operation and Development (OECD) (1980), *Guidelines Governing the Protection of Privacy and Transborder Data Flow of Personal Data*, OECD, Paris.

- Oz, E. (1994), "Barriers to international data flow", *Journal of Global Information Management*, Vol. 2 No. 2, pp. 22-9.
- Pearson, H.E. (1991), "Data protection in Europe", *The Computer Lawyer*, Vol. 24, August.
- Perrin, B. (1992), "Beatty proposes five privacy principles and kicks off public consultation process", *Canada NewsWire*, 29 June.
- Ratcliffe, M. and Waltz, M. (1992), "Easing data transfers across borders: European laws can present roadblocks", *MacWeek*, Vol. 2, November.
- Reidenberg, J.R. (1992), "Colloquium: the privacy obstacle course: handling barriers to transnational financial services", *Fordham Law Review*, Vol. 137, May.
- Roche, E.M. (1992), *Managing Information Technology in Multinational Corporation*, Macmillan, New York, NY.
- Rothfeder, J. (1992), "E-mail snooping", *Corporate Computing*, Spring, pp. 168-74.
- Rule, J.B. (1974), *Private Lives and Public Surveillance: Social Control in the Computer Age*, Schocken Books, New York, NY.
- Samiee, S. (1984), "Transborder data flow constraints: a new challenge for multinational corporations", *Journal of International Business*, Spring/Summer, pp. 144-50.
- Sardinas, J.L. and Sawyer, S.M. (1983), "Transborder data flow regulation and multinational corporations", *Telecommunications*, November, pp. 59-62.
- Shackleton, V.J. and Ali, A.H. (1992), "Work-related values of managers: a test of the Hofstede model", *Journal of Cross-Cultural Psychology*, Vol. 21 No. 1, pp. 109-18.
- Shils, E. (1979), "Privacy in modern industrial society", in Bulmer, M. (Ed.), *Censuses, Surveys, and Privacy*, Macmillan, London.
- Sieghart, P. (1984), "Information privacy and the data protection bill", in Bourn, C. and Benyon, J. (Eds), *Data Protection: Perspectives on Information Privacy*, University of Leicester, Leicester.
- Taylor, E.B. (1877), *Primitive Culture: Researches into Development of Mythology, Philosophy, Religion, Language, Art, and Custom*, Henry Holt, New York, NY.
- Turn, R. (Ed.) (1979), *Transborder Data Flows: Concerns in Privacy Protection and Free Flow of Information*, No. 1, American Federation of Information Processing Societies, Washington, DC.
- United Nations Centre on Transnational Corporations (UNCTC) (1981), *Transnational Corporations and Transborder Data Flow: An Overview*, UNCTC, Geneva.
- Waples, E. and Norris, D.M. (1992), "Information systems and transborder data flow", *Journal of Systems Management*, Vol. 43 No. 1, p. 28.
- Westin, A.F. (1967), *Privacy and Freedom*, Atheneum, New York, NY.
- Wigand, R.T. (1985). "Transborder data flow: its impact on business and government", *Information Management Review*, Vol. 1 No. 2, Autumn, pp. 55-65.
- Woody, C.V. and Fleck, R.A. (1991), "International telecommunications: the current environment", *Journal of Systems Management*, Vol. 42 No. 12, pp. 32-6.
- Yue, S.Y. (1992), "Hong Kong: call for new body to oversee data protection", *South China Morning Post*, 16 November.

(All correspondence related to this article should be addressed to Rita N. Walczuch, Institute für Internationales Management, der Karl Franzens Universität Graz, Merangasse 70/111, 8010 Graz, Austria.)