TRANSBORDER DATA FLOW: EU DIRECTIVE AND IMPLICATIONS FOR INTERNATIONAL BUSINESS

Elizabeth Longworth
Privacy Consultant and Lawyer
New Zealand

ABSTRACT

The knowledge economy leverages off the use of information, including personal data. The advent of global networks, such as the internet, now makes it possible to collect, process and transmit personal data on an unprecedented scale. This can be high volume use, such as in the form of the transfer of databases, or multiple one-off collections and exchanges from activities such as web browsing on the internet. The European Union Privacy Directive (1995) contains certain standards of privacy protection. It imposes export restrictions by prohibiting the transfer of personal data to countries which do not have privacy laws meeting the standards set out in the Directive or otherwise adequate levels of protection for those personal data. This constraint on transborder data flows from Europe could have far-reaching effects on those businesses in third countries that rely on continued access to personal data originating in Europe. The cost of various compliance mechanisms (such as tbdf contracts), and the need to build consumer trust and confidence, may make the economics and efficiency of third countries implementing their own domestic privacy laws, increasingly attractive.

1. TBDF ORIGINS AND CONCERNS

The phrase "transborder data flow" (or tbdf) was coined in the early 1980s in response to European privacy concerns. There was a growing awareness of the power of information as a resource, and of the increasing volumes of personal information (or data) that was flowing between countries, transborder.

Data transfers or "tbdf" may include the supply or exchange of personal information between business units or divisions within the same organisation, or where one entity is providing data processing services to another, or where the transfer of personal information is ancillary to a commercial arms-length transaction. The most intensive forms of tbdf occur in the area of human resources, financial records (banking, insurance, credit), customer related information (such as for marketing and travel reservations), and public sector agencies (law enforcement, border controls and tax agencies). With the high use of the internet, a significant amount of tbdf also occurs from web browsing activities. The use of digital
technologies facilitates electronic and on-line data transfers.

The European debate was focussed on the need to place some parameters on the widespread flow and use of the personal data of European citizens. During the early 1980s I was working in the privacy field in North America where the European initiatives on tbdf were being viewed with some alarm; the movement to constrain tbdf was sometimes likened to a form of "non-trade tariff barrier". The different perspectives on the best way to manage this issue (of the need for privacy protection) persists to this day; in particular, as evidenced in the different approaches taken by the European Union countries and the United States.

The European concerns culminated in the 1995 European Union Data Protection Directive (95/46EC), on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1 (discussed later.) This Directive required Members of the European Union to implement their own national privacy laws to reflect the data export restrictions in the Directive.

The most significant issue for the purposes of this discussion is the requirement in the Directive that data transfers from an EU Member country to a "third country" (outside the EU) can only take place where that country ensures an "adequate level of protection" (Article 25(1)). This gave rise to a very real concern as to the impact of such a constraint on those organisations within EU countries that need to export or supply personal data to organisations in third countries. What if that country does not have any privacy laws or what if its laws fail to satisfy the European Union "adequacy" test?

The significance of these issues has been exacerbated by the "information era". Over the past twenty years, personal data have increasingly been treated as key business commodities and assets. The knowledge economy leverages off the use of information, including personal data. The increasing capacity and sophistication of information communications technologies (ICT) are resulting in the globalisation of international data transfers. The advent of global networks, such as the internet, now make it possible to collect, process and transmit personal data on an unprecedented scale. This can be high volume use, such as in the form of the transfer of data bases, or more multiple one-off collections and exchanges from activities such as web

---

browsing on the internet.

2. EU ADEQUACY REQUIREMENT

The impact of the EU Directive was to make it mandatory for EU Member countries to prohibit the transfer of personal data to any country which does not have privacy laws meeting the standards set out in the Directive; it is a form of export restriction. The EU Members were required to make changes to their national laws to implement the Directive by October 1998. Since that date, there have been numerous other developments in Europe which reinforce the data protection impact of the Directive.

Although oversight is provided by the supervisory authorities of each Member country (such as the privacy office or data protection commissioners), it is also possible for any European citizen to lay a complaint about either a failure to implement the Directive or in respect of a proposed data transfer to a third country where the complainant believes the data will not be adequately protected.

The transfer of personal data to third countries is governed by Article 25 of the Directive. It states that,

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question."

The adequacy test is found in Article 26,

1. By way of derogation from Article 25 and save where otherwise provided by
domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

- the data subject has given his consent unambiguously to the proposed transfer; or
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
- the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
- the transfer is necessary in order to protect the vital interests of the data subject; or
- the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorise a transfer or a set of transfer of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

On the issue of adequacy, the Article 29 Working Party\(^2\) has provided various criteria by which the effectiveness of a privacy solution or data protection system (to implement the substantive privacy obligations) can be measured or adjudged; see Discussion Document, adopted by the Working Party on 26 June 1997, on First Orientations on Transfers of Personal Data to Third Countries – Possible Ways Forward in Assessing Adequacy.\(^3\) These criteria are summarised in the following extracts drawn from another paper which I wrote for the 22nd International Conference on Privacy and Data Protection (Venice, September 2000) on the subject of contractual privacy solutions. This is turn drew on a report which I wrote for the OECD (declassified 2000) on the subject of Transborder Data Flow Contracts in the Wider Framework of Mechanisms for Privacy Protection on Global Networks\(^4\).

The first criterion is the, "ability of the system to deliver a good level of..."
compliance with the rules”. This is characterised by the following factors:

- A high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them;
- The existence of effective and dissuasive sanctions;
- The existence of systems for direct verification by supervisory authorities, auditors or independent data protection officials.

The second criterion to measure the effectiveness of a data protection system is the level of, "support and help to individual data subjects in the exercise of their rights". There are a number of factors relevant to this measure. These include:

- A rapid and effective means of redress for the individual;
- The cost of redress (for the individual) should not be prohibitive;
- A complaints referral mechanism. The individual should know who to contact for the purpose of a data challenge. This presumes that the data subject has become aware of the transfer of and the subsequent reuse or disclosure of those data;
- Some form of institutional mechanism for the independent investigation of complaints. This is seen as preferable to other complaints options;
- Mutual recognition or assistance between supervisory authorities to facilitate investigations, where data have been transferred to a third country. The tbdf contract or system can provide for an independent expert nominated for this purpose (whether the supervisory authority or an agent, such as specialist auditors);
- Dispute resolution mechanisms which are timely and readily accessible to the data subject, and which can be tailored to the particular characteristics of privacy disputes.

The third criterion put forward by the Article 29 WP was the need to provide “appropriate redress” or a legal remedy to the aggrieved data subject. This requires:

- The right to have a complaint adjudicated by an independent arbiter;
- Some form of remedy for the data subject, such as compensation and/or injunctive or declaratory orders;
- The availability of appropriate dispute resolution mechanisms, and for these arrangements to be prescribed at the time of contract formation.

If the requisite level of privacy protection is viewed on a sliding scale, it is possible to summarise those elements which afford the greatest level of privacy protection:

- The starting point is specific reference to substantive rules which set out the parties' privacy obligations. The inclusion of this element is "non-negotiable", unlike some of the other elements.
- Some means of ensuring accountability and verifying that the parties are complying with their privacy obligations. This element is viewed by some as one of the variables, in that its necessity may depend on the quality of the other elements.

---

5 Accountability Principle 14 "A data controller should be accountable for complying with measures which give effect to the principles stated above", OECD Privacy Guidelines
privacy protection measures being adopted within, or ancillary to, the contract.

- Irrespective of the verification process, there must be a stand-alone workable complaints and investigations process, in the event that there is a breach of the privacy obligations.
- The provision of appropriate dispute resolution mechanisms, not just for contracting parties but which also contemplate a complaint by the data subject and (if applicable) the potential involvement of any applicable data protection authority, government supervisory agency or third party certification organisation.
- The privacy and implementation obligations must be enforceable, with recourse to an independent arbiter and the availability of sanctions.

In its discussion on criteria for assessing adequacy, the Working Party stressed the need for a case-by-case approach, and that the adequacy test also envisages the possibility of ad hoc solutions, notably of a contractual nature. It discussed a proposal for the development of a "white list" of third countries which could be assumed to ensure an adequate level of protection. It clarified that it is not only the content of the rules applicable to tbdf that is important, but also the procedural mechanisms in place to ensure the effectiveness of such rules.

Most importantly, the Working Party included a list of categories of data transfers which it considered could pose particular risks to privacy. It can be assumed that these categories are still relevant and the development of appropriate privacy protection mechanisms for such data should be a priority for third countries. They are:

- Transfers involving certain sensitive categories of data as defined by Article 8 of the Directive;
- Transfers which carry the risk of financial loss (eg credit card payments over the Internet);
- Transfers carrying a risk to personal safety;
- Transfers made for the purposes of making a decision which significantly affects the individual (such as recruitment or promotion decisions, the granting of credit, etc);
- Transfers which carry a risk of serious embarrassment or tarnishing of an individual's reputation;
- Transfers which may result in specific actions which constitute a significant intrusion into an individual's private life such as unsolicited telephone calls;
- Repetitive transfers involving massive volumes of data (such as transactional data processed over telecommunications networks, the Internet etc.);
- Transfers involving the collection of data in a particularly covert or clandestine manner (eg Internet cookies).

The Working Party has issued various opinions interpreting the provisions of the above Articles (25 and 26). It has also addressed the issue of industry self-regulation in a Working Document adopted on 14 January 1998, *Judging Industry Self-Regulation: When Does it Make a Meaningful Contribution to the Level of Data
Protection in a Third Country? In the context of self-regulatory instruments, such as industry or professional codes, the Working Party refers to the same adequacy criteria of compliance, support and help for data subjects and redress mechanisms.

The Working Party also commissioned a study by which a methodology was developed for adequacy assessments (see Final Report – Application of a Methodology Designed to Assess the Adequacy of the Level of Protection of Individuals with Regard to Processing Personal Data: Test of the Method on Several Categories of Transfer, September 1998). This Report covered the categories of human resources data, sensitive data in airline reservations, medical and epidemiological data, electronic commerce data and sub-contracted data processing. The conclusions reflect the need to evaluate these categories in the context of their own industry mechanisms and information practices. The Report highlighted the difficulties of drawing broad conclusions or generalisations, given the very different circumstances applying to different categories of data.

The most recent opinion of the Working Party is Opinion 1/2001, adopted on 26 January 2001, called "Draft Commission Decision on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries under Article 26(4) of Directive 95/46". The significance of this work is that it recognises that adequacy need not only be satisfied by the existence of appropriate privacy legislation in the third country, but may also be achieved by certain mechanisms, such as the use of tbdf contracts.

3. TBDF CONTRACTS

Although the Working Party originally considered that Article 25 would require a case-by-case approach to assess the adequacy of the circumstances surrounding each set of data transfers, it is now recognised that mechanisms need to be developed to rationalise the decision-making process for large numbers of individual transfers. The role of contract, as a means of ensuring adequate privacy protection, is expressly recognised in the Directive (see Article 26(2)).

To the extent that the national or domestic privacy law of the EU Member also

---

6 http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp7en.htm
provides for privacy protection through the use of contract, then the data export may be regulated by the use of a tbdf contract. However, in order for such contracts to be "approved" as providing an adequate level of privacy protection, it is necessary for there to be some template or standardisation of tbdf contracts. This need has led to a significant amount of work to develop model contract clauses. These have evolved as follows. The early focus of what is known as "contractual privacy solutions" was on conventional business-to-business (B2B) data transfers, as opposed to what is now known as business-to-consumer (B2C) tbdf (in the context of internet usage).

The first significant work was the 1992 Council of Europe Model Contract (to ensure equivalent data protection in the context of transborder data flows). These clauses were revised by the International Chamber of Commerce (ICC) in the light of the changing standard within the EU Directive from the draft requirement of "equivalent protection" to the current reference to "adequate protection". This work incorporated the comments of the Article 29 Working Party. The result was the ICC Model Clauses (for use in contracts involving transborder data flows). These have in effect been superseded by the January 2001 Standard Contractual Clauses.

There have been other initiatives on the use of model contracts for B2B data transfers, including the Working Document adopted by the Article 29 Working Party of the European Commission on 22 April 1998 containing "Preliminary views on the use of contractual provisions in the context of transfers of personal data to third countries." The most recent work on tbdf contracts is probably the European Commission proposal on Standard Contractual Clauses, Draft Version dated 19 January 2001 (see above). These clauses try to address some of the issues previously identified by the Working Party and others on the shortcomings of tbdf contracts; for example, the difficulty of providing redress for the data subject if the individual is not a party to the contract between the data exporter and importer, or where there is no law recognising the rights of third party beneficiaries. The clauses proposed by the European Commission, in the Draft Opinion or Decision, are intended to be re-evaluated after three years experience with their operation.

The Working Party has clarified that even if the European Commission has recommended certain contractual clauses as offering sufficient safeguards, the data transfer will still be subject to the national or domestic legislation of the relevant Member country. Therefore, the lawfulness of the processing operation will be subject to the conditions or the way in which the applicable national legislation has implemented the provisions of the Directive. It should be noted that the privacy laws of some EU countries do not recognise tbdf contracts.

The fundamental provision within the European Commission Standard Contractual Clauses is the requirement on the data importer to agree and warrant to process the personal data received from the EU Member in accordance with certain processing conditions that will provide adequate safeguards within the meaning of Article 26(2) of the Directive. In particular, "The Working Party would like to stress the fundamental and indispensable character of three of these conditions in order to guarantee a minimum level of protection: the purpose limitation principle, restrictions on onward transfers and the data importers' undertaking of providing the data subjects with the rights of access, rectification, deletion and objection arising from the Directive 95/46/EC."\(^\text{10}\)

4. TBDF IN THE ON-LINE WORLD

The advent of the internet has exacerbated the threat to personal privacy. The use of this technology in C2B (consumer to business) tbdf poses particular problems in terms of privacy protection, especially where it involves the collection of personal data from individuals or consumers in a way which is outside their knowledge or beyond their control. The significance of the problem has been recognised by the linkages being made between building consumer trust (such as through effective privacy protection) and the facilitation of electronic commerce.

In the on-line world, the nature of C2B interactions is such that often there will be no pre-existing relationship between the participants; the web browsing may be random, with many first time or intermittent site visits. The exception is where the consumer has an established relationship, such as a history of ordering goods on-line from a particular business or of applying for credit. The participants will also be removed from each other in terms of distance, time and geographical location.

\(^{10}\) http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp38en.pdf
Despite this separation, the technical features of the medium are designed to facilitate data transfers. The disclosure of data is made possible through web browsing software which provide the means to identify the network and machine used to access the web, the URLs of previously visited sites, and by matching the information derived from the use of "cookies". The data collection and storage is facilitated by caching and the availability of search engines, robots and internet indexes.

The more overt data collection occurs when the consumer provides personal details in the course of a web site interaction, whether of credit card and other payment details, contact details, personal preferences and so on. In transactions to acquire goods and services, the data transfer is usually incidental to the primary purpose.

When an individual (a consumer) merely visits a web site, the browsing activity can also generate data. This is a form of data transfer; it is likely to be transborder. However, the consumer has not ordered any goods or services, but has been merely viewing and perhaps downloading information; the consumer is "window-shopping". It is unlikely that contractual requirements such as an intention to be bound, or offer and acceptance analysis, would apply to what is in essence only a communication or interaction. This characteristic of online C2B interactions requires that any attempt to protect the privacy interests of the consumer must begin prior to any contractual stage. The use of tbdf contracts for C2B may not be possible nor appropriate.

This means that in the context of C2B transfers, there is an important role for measures such as model privacy protection policies. There is a need to bring privacy protection issues to the consumer’s attention at the earliest possible stage in the web site interaction. It will be too late to afford the consumer any genuine freedom of choice as to the transfer of these data if notification of the uses to which personal data may be put takes place only at the stage when a contract for the supply of goods or services is concluded.

There are some encouraging developments in this regard. Recently I completed another assignment for the OECD on electronic commerce codes of conduct. It is interesting to note that of the 29 B2C e-commerce codes studied for the Report, every code addressed the issue of privacy protection. It is not possible to draw any conclusions as to the adequacy of the privacy provisions within each code; however, it
is interesting to note that the drafters of these codes recognised the need to incorporate privacy protection policies in the context of electronic commerce transactions.

Where privacy protection policies are incorporated into a C2B contract, the consumer will be entitled to take action to enforce these as a term of the contract. The legal status of privacy protection policies or statements generally is less clear and there may be limited prospect of enforcement by an individual consumer. Depending on national laws, the consumer might have a cause of action for misrepresentation or recourse under trade practices or consumer protection laws. Despite these possibilities, there are serious practical impediments in the way of any individual consumer that attempts to issue proceedings against a business which is operating on the web, given the amount of resource such actions require. There would be the difficulties of determining which court has jurisdiction, assuming it is even possible physically to locate the entity which has responsibility for the web site content or the information use and disclosure practices associated with that site.

For those C2B transfers which are structured so as to form a contract, the outcome of the various initiatives on the contract requirements for electronic commerce transactions will be directly applicable to online C2B privacy contracts. These initiatives include the legal recognition of authentication measures (such as the use of electronic and digital signatures) and rationalising the evidentiary requirements. There is also on-going work to resolve conflicts of laws (choice of law and jurisdiction) in transborder transactions.

5. JURISDICTIONAL ISSUES

The globalisation of commerce, including tdft, means that increasingly transactions involve parties from more than one country or involve obligations to be performed in more than one country. This gives rise to significant choice of law questions and issues such as: where will the dispute be determined? is effective interim relief available, pending trial? And, will a judgment obtained in one jurisdiction be enforceable elsewhere, either against the assets of the defendant or against the defendant personally?

The problem of reconciling the above conflict of laws issues for on-line interactions, whether in the context of electronic commerce generally or specifically
in respect of transborder data flows, remains unsolved. This is a major issue of the present day electronic environment; it is receiving close scrutiny by a number of international fora. In any international contract it is essential to prescribe which governing laws and jurisdiction should apply to that contract. Transborder data flow contracts have the same need. Even if the parties to the contract apply some contractual foresight, this does not resolve the numerous difficulties of enforcing a foreign judgment or of applying the rules to the peculiarities of an internet interaction.

There are many participants in a C2B transfer. The internet has many intermediaries, whether in the form of service providers or in the way the technology operates (utilising servers to host the web page files, the routing of data packets through nodes around the world, and the practice of caching). Each participant or activity may be "located" in different legal jurisdictions. The question, therefore, is which country's substantive legal rules should apply to a data transfer, message content or other activity, accessed via the internet? Whose courts would have jurisdiction to adjudicate civil disputes and prosecute breaches? Clearly, the presumptions of physical location and proximity (which are inherent in the linking of territoriality to geographical borders) are fundamentally challenged by the characteristics of global networks.

The choice of law (prescribing the governing or proper law of the contract) will be highly significant in the adaptation and uptake of tbdf contracts. Although a forum may have personal jurisdiction and venue, the choice of law rules may require that the dispute be heard under the substantive law of another jurisdiction. Each country has its own private international law (forming part of its national or domestic law). These variances between countries are what distinguishes each body of private international law from public international law. Despite these differences, there are on-going efforts to harmonise the rules of conflict of laws. Many jurisdictions pursue common objectives and are influenced by the doctrine of comity and the need to respect the civil justice systems of other countries.

The question of when and where a contract is concluded is a major factor in determining which legal system is to govern the particular transaction. Where transactions are conducted over the internet, the question is not always easy to answer. The Global Top Level Domain name .COM gives no indication where a business is located. Even where the name uses a country code such as .DE or .UK, there is no
guarantee that the business is established in that country. Key characteristics of the internet are its re-routing ability and anonymity features.

In general, it is provided that contracting parties are permitted, subject to a criterion of reasonableness, to select which legal system will govern a particular transaction. Linked to this is the question which national courts will have authority to rule on the interpretation of the contract. Where parties are resident in different countries, for example, in Canada and Germany, it would be open to them to provide that the contract should be governed by Canadian law but that any disputes should be brought before the German courts.

Within Europe, the Brussels and Rome Conventions\textsuperscript{11} provide for partial exceptions in the case of consumer contracts. The latter provides that a supplier with a "branch, agency or establishment" in the consumer’s country of residence is to be considered as domiciled there. Consumers may choose to bring actions in either their country of domicile or that of the supplier, while actions against the consumer may be brought only in the consumer’s country of domicile. The question whether an internet-based business can be regarded as having a "branch, agency or establishment" in all the countries from which its facilities may be accessed, is uncertain.

The Brussels Convention builds on the Rome Convention’s provisions and provides that an international contract may not deprive the consumer of ‘mandatory rights’ operating in the consumer’s country of domicile. The scope of mandatory rights is not clear-cut, but given the emphasis placed on the human rights dimension in many international instruments dealing with data protection, it is arguable that any contractual attempt to deprive consumers of rights conferred under the Council of Europe Convention and the EU Directive, would be declared ineffective on this basis.

More recent developments may complicate matters. It has been proposed that, within the European Union, transactions entered into by electronic means should be regulated by the law of the supplier. (I am unsure as to the current implementation status of what was a draft EU Directive on electronic commerce.) This approach is justified on the basis of supporting the development of the e-commerce new industry. There appears to be an inescapable tension between choice of law provisions designed

to favour the development of electronic commerce (by making the nature of the liabilities incurred by service providers more predictable) and those consumer protection policies which give priority to the interests of consumers, (by maximising their access to local courts and tribunals).

There is a clear link between privacy and electronic commerce. The volume and nature of data transfers occurring in electronic commerce transactions is prompting privacy concerns. The lack of consumer trust and confidence in the level of protection afforded personal data, by the internet, is an inhibiting factor in the growth of electronic commerce. Yet, privacy protection (and the ability of data subjects to obtain redress) has its origins in human rights conventions and is also clearly a consumer protection issue. This tension will need to be reconciled. The issue is how much autonomy should the participating parties have to determine their choice of law and jurisdiction, if this adversely affects the data subject's need to have access to appropriate redress mechanisms. Even if the data subject can access a local court, there remains the problem of enforcing judgment.

I am grateful to David Goddard, Barrister, New Zealand for the following update on this jurisdictional issue. Work was commenced in 1992 by The Hague Conference on Private International Law to draft a new convention on jurisdiction and judgments in civil and commercial matters. The proposed approach was to specify some agreed grounds of jurisdiction, and some prohibited grounds, but otherwise to leave the question to the law of each Convention country. Judgments falling within the agreed grounds of jurisdiction would be enforceable in all other Convention countries. Where one Convention country exercised jurisdiction in the "grey" area, it would be a matter for each other Convention country to decide whether or not to recognise and enforce the resulting judgment. The Convention would extend beyond money judgments to injunctions and other forms of relief, and could embrace interim orders as well as final judgment.

If the drafting work eventuates into a ratified Convention, it will solve one of the most frequently occurring problems of private international law, which causes considerable delays and unnecessary cost in many cross-border disputes. The

---

12 Revised version of a paper presented by David Goddard, Barrister, Wellington, to the New Zealand Law Conference in Rotorua, April 1999, Global Disputes – Jurisdiction, Interim Relief and Enforcement Of Judgments
alternative may be for countries such as New Zealand and others in Asia to consider acceding to the Lugano Convention which (unlike the Brussels Convention, which is restricted to EU Members) is open to accession by all countries. This would simplify questions of jurisdiction and enforcement of judgments as between the signatories and most European countries, including the United Kingdom.

As Goddard points out, an integral part of facilitating global commerce is facilitating the resolution of cross-border disputes, by reducing uncertainty and costs in connection with the selection of a forum, interim relief, gathering evidence and enforcement of both interim orders and final judgments. New Zealand law does not make adequate provision for these matters; no doubt this is also the case in other countries in the region. The absence of adequate provision for such matters is of particular concern between countries where there are close commercial links and the movement of people, business and data on a regular basis. Any coherent approach to legislating for increased globalisation of trade, including tbdf and electronic commerce, means that such issues should be an integral component of legislative reform.

The impediments to relying purely on recourse under a tbdf contract are the reason why contracts are relying on ancillary mechanisms, such as looking to a data protection authority or some other supervisory agency (government or industry) for remedies and sanctions. Other avenues that would be well worth pursuing would be the development of an online dispute resolution service which could provide first tier resolution for privacy disputes; in particular, where these are high volume and originate from individuals with insufficient resources to pursue their other legal remedies (if any). In a global economy, the need for an online privacy dispute resolution is going to grow rather than diminish.

6. BUSINESS IMPLICATONS FOR NON-EU COUNTRIES

The adequacy requirement of the Directive is a form of export restriction. It could yet prove to have far-reaching consequences for businesses in non-EU countries, such as in Asia, that need to obtain or use personal information or data which originate within an EU country. The European Commission is currently evaluating third countries in terms of the adequacy requirement, including working through a list
of countries in the Asia Pacific Region. For those countries which do not have any privacy legislation, or whose national privacy laws are significantly flawed (so as not to satisfy the adequacy test), the potential impact of these developments should not be underestimated.

The "new economy" relies on the ability to transmit information, including legitimate use of personal data. What will be the impact if, as a result of a complaint over a data transfer to a third country, an airline is unable to obtain a customer manifest, an insurance company is unable to access insurance records, a business is unable to access its human resources records, or a marketing division can no longer obtain its customers' profiles?

These examples all presume that the proposed use of the personal data exported from an EU country fulfils the purpose limitation and other principles of the OECD Privacy Guidelines. The fact of such compliance will be irrelevant, however, in the absence of appropriate national legislation to protect personal data in the third country (of the importer), or in the absence of contractual mechanisms (approved under the EU Directive) that fulfil the EU adequacy requirement.

There are other mechanisms for adequacy, such as voluntary codes of conduct and industry standards; however, experience shows that there are significant issues in meeting the content and procedural requirements of adequacy, including the need for enforcement (in the form of independent supervision, meaningful sanctions and a track history of proven compliance).

As is the case with any of the alternative mechanisms to national privacy legislation, there are significant economic costs and inefficiencies in a situation where the various mechanisms for tbdf require case-by-case analysis, and an approvals process to ascertain if the circumstances of the data transfer will meet the adequacy requirements under both the EU Member's privacy laws and under the EU Directive. The process to establish "adequacy" will be complex and lengthy, presumably requiring investigation of a number of test cases.

It could be argued that the compliance cost for third countries in satisfying the adequacy requirements by enacting their own national privacy protection laws, would be lower than the cumulative costs of requiring business and/or industry to fend for
themselves in trying to design suitable adequacy mechanisms. In addition to the arguments based on economics and efficiency, there is also the fact that privacy protection is a human right and goes to the heart of public confidence and consumer trust.