OECD publishing

Please cite this paper as:

OECD (2000-09-21), "Transborder Data Flow Contracts in the Wider Framework of Mechanisms for Privacy Protection on Global Networks", *OECD Digital Economy Papers*, No. 66, OECD Publishing, Paris.
http://dx.doi.org/10.1787/233311170363

OECD Digital Economy Papers No. 66

Transborder Data Flow Contracts in the Wider Framework of Mechanisms for Privacy Protection on Global Networks

OECD

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

OLIS : 21-Sep-2000
Dist. : 22-Sep-2000

Or. Eng.

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

DSTI/ICCP/REG(99)15/FINAL
Unclassified

Working Party on Information Security and Privacy

TRANSBORDER DATA FLOW CONTRACTS IN THE WIDER FRAMEWORK OF MECHANISMS FOR PRIVACY PROTECTION ON GLOBAL NETWORKS

95592

Or. Eng.

PREFACE

The Report on Transborder Data Flow Contracts in the Wider Framework of Mechanisms for Privacy Protection on Global Networks builds on the commitment of the OECD Member countries at the 1998 Ottawa Conference "A Borderless World: Realising the Potential of Global Electronic Commerce", to encourage the use, and development, of model contractual solutions for online transborder data flows, and to ensure that effective enforcement mechanisms are available both to address non-compliance with privacy principles and policies and to ensure access to redress.

The report discusses the use of transborder data flow (TBDF) contractual solutions in the wider framework of mechanisms for privacy protection, and recognises the changing environment for TBDF and the impact of the global information infrastructure (GII) on the processing and transmission of personal data. It examines the two main categories of transborder data flows; business to business (or B to B), and consumer to business (or C to B), and highlights the issues raised by applying contractual analysis and structures to online communications, in particular to C to B communications. The report also stresses the need for developing tailored dispute resolution mechanisms for C to B online interactions. Where appropriate, the report suggests possible further initiatives to foster the widespread use of contractual privacy solutions for TBDF in online communications.

It is hoped that the report will assist in developing a common understanding of the use of contractual solutions in the wider framework of privacy protection mechanisms. Other mechanisms exist, ranging from privacy laws to self-regulatory frameworks (such as codes of conduct or practice and formal industry standards) that also enhance online privacy protection. These mechanisms include privacy enhancing technologies (PETs), online educational tools, systems for labelling, certifying and attaching privacy seals, and dispute resolution mechanisms.

Following the procedure agreed at the 37th Session of the Committee for Information, Computer and Communications Policy (ICCP), the Working Party on Information Security and Privacy agreed at the end of July 2000 to recommend to the Committee the declassification of the report under a written procedure. The ICCP Committee subsequently approved the declassification of the report on 15 September 2000.

The report, prepared in collaboration with a number of experts and consultants under the supervision of the OECD Secretariat, incorporates contributions from Member countries, international and regional organisations and the Business and Industry Advisory Committee (BIAC). In particular, the Secretariat wishes to thank Elizabeth Longworth, Lawyer, Principal of Longworth Associates, New Zealand who drafted the first version of the report, and recognises the contributions received from Lorraine Brennan, Director of Arbitration and Intellectual Property, and Legal Counsel, US Council for International Business, Alexander Dix, Data Protection and Access to Information Commissioner for Brandenburg, Germany, and Ian Lloyd, Professor of Information Technology Law and Director of the Centre for Law, Computers and Technology at the University of Strathclyde, United Kingdom.

TABLE OF CONTENTS

MAIN POINTS

Fundamental requirements for contractual solutions

A number of fundamental requirements for privacy contractual solutions, as well as additional relevant factors such as constraints or ancillary requirements and other privacy protection mechanisms, are considered important in promoting privacy compliance. Among these requirements are the substantive rules -- the minimum level threshold being the Principles in the OECD Privacy Guidelines -- which set out the parties' privacy obligations; a workable complaints and investigations process, and the provision of appropriate dispute resolution mechanisms. The substantive rules proposed in the report are intended to serve as a common reference for the discussion of and conditions for what is currently in use or under development, the experience to date, and possible further work in respect of contractual approaches.

Contractual models currently in use or under development

The report highlights the historic focus on TBDF contracts for B to B transfers and examines model contracts, notably the model clauses developed by the International Chamber of Commerce (ICC), as well as current initiatives aimed at using codes of conduct and formal industry standards as a form of contract. It draws attention to the flexibility of model contracts, which allow the modification of the detail of their provisions to accommodate categories of industries/sectors as well as other particular circumstances, such as specific data or the use of a particular medium. While identifying certain constraints on the use of B to B contracts, the discussion recognises the potential of model B to B contracts to satisfy privacy protection expectations regardless of whether or not the transfer occurs in an online or offline environment, in particular with the support of ancillary measures such as online privacy notices to the individuals at the point of data collection.

Recourse of the individual in B to B contracts

Redress for breach of contract is available to the parties to the contract and usually also to third-party beneficiaries of the contract. To ensure that data subjects have the means to enforce a B to B TBDF contract, the ICC Model Contract provides the data subject, or a Data Protection Authority on behalf of the data subject, the right to bring an action for breach of contract against the data exporter for any alleged breach of the data importer under the contract. This ensures that the data subject has a party (the data exporter) to hold accountable in his/her home country. While some express concern that this remedy might not be sufficient to secure compliance by the data importer, it is important to note that the Data Subject may also have enforceable rights through other privacy protection infrastructures such as laws or effective self-regulation.

Issues with Consumer to Business interactions

The report considers the characteristics of C to B online interactions, discusses the issues raised by applying contractual analysis and structure to such interactions, and demonstrates privacy issues which

arise prior to the conclusion of a contract, calling for other privacy protection mechanisms in such cases. It therefore suggests that privacy protection policies and statements have a significant role to play and that they may provide the means to transform a privacy policy into a binding commitment. Consumer protection agencies, third party organisations, and effective internal organisation review mechanisms are identified as having a significant role to play in providing certification or verification services and tools.

The need for appropriate dispute resolution mechanisms

The issue of dispute resolution is identified as a critical one to build trust in the use of global networks for both businesses and consumers. It is suggested that complaints, investigation, dispute resolution and enforcement mechanisms should be developed in such a way as to address the specific characteristics of C to B online transfers. In that respect, conventional methods of dispute resolution are discussed and their benefits and limitations highlighted. Other current experience of online dispute resolution mechanisms is also presented.

Future initiatives

Finally, the report draws a number of conclusions from the discussion of the above topics. It highlights particular issues to be resolved in order to satisfy the privacy protection objective. The report also seeks to identify: initiatives which could foster the use of privacy contracts; any other matters which require further consideration or investigation; initiatives which could advance the work to date on the use of contractual solutions, especially for on-line C to B transfers and interactions; and the need for any specific online dispute resolution service tailored for C to B transfers.

The following four themes emerge from the report:

- The importance of promoting privacy awareness and providing educative tools.

  In accordance with the Openness Principle of the OECD Privacy Guidelines, there should be continued emphasis on systemic measures to improve privacy notice and consent procedures such as the OECD Privacy Policy Statement Generator. There may be an opportunity for a dedicated information page to catalogue resources to obtain additional information regarding privacy protection laws, self-regulatory mechanisms, etc.

- How to develop enforceable privacy commitments for online C to B transfers.

  Privacy policy statements could be used in the future, as a basis for establishing the terms and conditions governing the transactions on a Web site. In particular, they could address the substantive privacy rules, any verification measures or certification processes applying to the Web site. The consumer would be notified of these terms and conditions prior to the point in time at which the contract is entered into.

- The various international developments which require monitoring and further collaboration.

  There are many international developments which need to be monitored so that it is possible to learn from these experiences when implementing contractual privacy solutions and ancillary measures. Such developments include any further work based on the ICC Model Clauses or the various projects around the world to develop online dispute resolution measures.

- The potential to develop a framework for effective alternative dispute resolution for online C to B transfers.

1. INTRODUCTION

Globalisation of data transfers and impact of the Internet

The advent of the global economy, and the increasing sophistication of information and telecommunications technologies, are resulting in the globalisation of international data transfers. International information systems are the basic infrastructure of a multinational company's operations in trading goods and services. More and more companies are moving data between countries. Organisations who have control over the collection and processing of personal data, have the means to reuse and transfer those data on an unprecedented scale. This can be high volume TBDF, such as in the form of databases, or multiple one-off collections from activities such as Web browsing on the Internet.

The network of networks that comprises the global information infrastructure is facilitating this transformation in transborder data flows. The GII involves the interconnection of "information highways", comprising telecommunications and computer technologies. The Internet is the most obvious example of these global networks. The online environment provides great benefits to users such as tailored and interactive information, products and/or services and enhanced privacy and security including use of encryption, firewalls, and identification procedures that extend beyond what is used in pre-Internet commerce, but it also creates new challenges for privacy protection.

Consumer trust and e-commerce

In this global trade environment, personal data is growing in economic significance. The information economy (now the knowledge-based economy), leverages off the use of information, including personal data. Data are seen as key business assets.

The nature of the challenge has been recognised both internationally and by national governments. This is illustrated by the linkages which have been made between building consumer trust (such as through effective privacy protection) and the facilitation of electronic commerce. This was one of the themes of the OECD Member countries' 1998 Ottawa Conference on "A Borderless World: Realising the Potential of Global Electronic Commerce". The result was a commitment to ensure privacy protection on global networks and, notably, to encourage the use and development of model contractual solutions for on-line TBDF.

The role of contracts in the wider framework of privacy protection mechanisms

Internationally, there are many different mechanisms for enhancing privacy protection. These range from privacy laws to self-regulatory frameworks (such as codes of conduct or practice and formal industry standards). Other mechanisms include privacy enhancing technology (PET) and systems for labelling, certifying and attaching privacy seals. Contracts have their place among these mechanisms.

Contracts are intended to be binding agreements, enforceable in law. Used for TBDF, they can provide a degree of flexibility and can accommodate some of the differences between countries, in the way they approach privacy protection in the context of global networks. Contracts may also be a practical and positive measure where there are different or no data protection laws or effective self-regulation regimes. They may also complement or support compliance with a privacy self-regulatory framework or statutory regime. It is possible for the terms and conditions of the contract to reflect the requirements of specific privacy instruments.

For example, some instruments require special treatment for transborder data flows. In particular, Part Three of the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* 1980 (OECD Privacy Guidelines) states that Member countries may restrict the flows of certain categories of personal data specifically controlled by their domestic legislation, to Member countries which have no "equivalent" protection. This restriction must be balanced with the OECD's stated determination to advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries.

A similar provision is contained in Article 12 of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) and Article 9 of the United Nations Guidelines Concerning Computerised Personal Data Files (1990). The European Union Data Protection Directive (95/46EC) also provides in Article 25(1) that those data transfers from a Member country to a third country can only take place where that third country ensures an "adequate level of protection". The possibility of using contracts to ensure that personal data transferred from one country to another receive "adequate protection" under the EU Directive is explicitly recognised by Article 26(2). In addition, for many years some national instruments have made provision for the special treatment of TBDF (*e.g.* Germany, France).

2. FUNDAMENTAL REQUIREMENTS FOR CONTRACTUAL SOLUTIONS

Any discussion on contractual solutions to protect privacy and personal data can be enhanced if there is a common understanding of the objectives of this type of solution. This includes an understanding of the role of contracts within the wider framework of privacy protection mechanisms and of those elements of contractual solutions which are considered important to protect privacy. In terms of TBDF contracts, it may be helpful to collate these elements, which are necessary to deliver an effective contractual solution. Any discussion should also consider ancillary requirements or features of the privacy framework within which the TBDF contract must operate.

Need for a common substantive reference

The parties to the TBDF contract need to ensure that there are substantive data protection rules, which apply to the data transfer. These rules could be a reiteration of the principles of the OECD Privacy Guidelines or drawn from some other instrument which sets out equivalent principles. Contractual privacy solutions can achieve an appropriate level of privacy protection, such as that articulated within the OECD Privacy Guidelines. This objective is qualified by the balancing exercise inherent in the preamble or introductory statement in the OECD Privacy Guidelines,

> *"Recognising:*
>
> > *that although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information;*
> >
> > *that automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices;*
> >
> > *that transborder flows of personal data contribute to economic and social development;*
> >
> > *that domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows;*
>
> *Determined to advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries".*

The OECD Privacy Guidelines[1] represent a consensus on fundamental requirements and objectives for privacy protection and an appropriate balance between effective privacy protection and the free flow of information. However, the appropriate level of privacy protection can also be drawn from other national law or self-regulatory frameworks, based on the OECD Guidelines.

For the European exporter, it could be the requirements as prescribed by the EU Directive or agreements between the European Commission and third countries. In that respect, the European Union advisory Working Party on the Protection of Individuals with regard to the Processing of Personal Data, ("Article 29 Working Party") has produced a Working Document[2] on the use of contractual provisions for TBDF to third countries. This document which assesses the meaning of "adequate safeguards" as used in the European Directive in relation to TBDF contracts, recognises that the obligations and rights set down in the OECD Guidelines, which are not dissimilar from other international instruments, express "a degree of consensus as to the content of data protection rules which stretches well beyond the fifteen states of the community".

Reference could also be made to codes of conduct and industry standards. For some years there have been self-regulatory moves to adopt such instruments for privacy protection. These measures can take the form of industry-specific or sectoral privacy codes of conduct (practice). They can be administered by the applicable supervisory body for that industry or sector, with the power to impose sanctions on its members or can be enforced by private sector self-regulatory bodies as is the case in the United States. They are a form of industry-wide contracts among participating members. In some jurisdictions, such as New Zealand, the privacy code is given statutory force and is subject to the jurisdiction of the supervisory data protection authority. These standards could be incorporated into TBDF contracts. Another form of consensual standard is that established by the official standards organisation at the national level. An example is the Canadian Standard CAN/CSA-Q830-96. This approach is particularly relevant for those countries which have no privacy laws or where private sector TBDF are not regulated in any way. Any of these can provide a minimum set of privacy principles, an implementation methodology, and a suggested structure within which to implement the privacy protection measure.

The flexibility afforded by the ICC Model Clauses, which recognise that the approach to data protection varies between countries, provides a means of building bridges between these approaches on the basis of the consensus expressed in the OECD Guidelines. Accordingly, the Clauses require the data importer to observe the rules on data protection applicable in the Member State where the data exporter is established, or if appropriate, a set of principles deemed to be adequate for transborder data flows. This means, by way of illustration, that the exporter (and therefore the importer) could be bound to comply with a detailed set of privacy principles as prescribed under the law of New Zealand or Hong Kong (if this is the country of the exporter). Conversely, there may be less comprehensive privacy regulations, or none at all, to be addressed in the privacy obligations of the parties to the contract. Despite the state of any applicable privacy law, the Model Clauses contain a separate obligation prohibiting the onward transfer of the data without the consent of the data exporter. This provides a proper basic level of privacy protection.

Need to ensure compliance with the substantive reference

In order for a contract to achieve effective privacy protection, a second important requirement is that the substantive rules that it includes will be given effect. Such a requirement is consistent with the accountability principle of the OECD Privacy guidelines, which requires that "a data controller should be accountable for complying with measures which give effect to the principles (…)". The Guidelines also provide that:

> *"Member countries should in particular endeavour to:*
> *(…)*
> *(d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; (…)"*

Tests for the effectiveness of a data protection system have been suggested, for example, by the Article 29 Working Party. They proposed the three following general criteria:

a) The ability of the system to deliver a good level of compliance with the rules, which includes a high degree of awareness among data controllers of their obligations, and among data subjects of their rights; the means of exercising them; the existence of effective and dissuasive sanctions; and systems for direct verification by supervisory authorities, auditors or independent data protection officials.

b) Support and help to individual data subjects in the exercise of their rights which includes a rapid and effective means of redress for the individual, and some sort of institutional mechanism allowing independent investigation of complaints.

c) Appropriate redress for the individual, which involves a system of independent adjudication or arbitration. Appropriate measures to ensure compliance with privacy rules can be provided for in a contract. For example, the ICC model contract gives the data subject or data protection Authority a right of action against the data exporter under the relevant law. The data exporter can then seek indemnification from the data importer for breach of contract.

An alternative approach can be found in the US discussion draft of January 1998 on "Elements for Effective Self-Regulation for Protection of Privacy"[3]. In that document, the test for an effective self-regulatory privacy regime is described as having to do more than articulate broad policies or guidelines: effective self-regulation involves substantive rules, as well as the means to ensure that consumers know the rules, that companies comply with them, and that consumers have appropriate recourse when injuries result from non-compliance.

As concerns enforcement mechanisms, an effective self-regulatory privacy regime should include mechanisms to assure compliance with the rules and appropriate recourse to an injured party when rules are not followed. Such mechanisms are essential tools to enable consumers to exercise their privacy rights, and should, therefore, be readily available and affordable to consumers. They may take several forms, and businesses may need to use more than one depending upon the nature of the enterprise and the kind of information the company collects and uses.

Such enforcement tools include notably consumer recourse (mechanisms by which consumers' complaints can be resolved), verification (attestation that the assertions businesses make about their privacy practices are true and that privacy practices have been implemented as represented), and consequences (failure to comply with fair information practices should have consequences. Among these may be cancellation of the right to use a certifying seal or logo, posting the name of the non-complier on a publicly available "bad-actor" list, or disqualification from membership in an industry trade association. Non-compliers could be required to pay the costs of determining their non-compliance. Ultimately, sanctions should be stiff enough to be meaningful and swift enough to assure consumers that their concerns are addressed in a timely fashion. When companies make assertions that they are abiding by certain privacy practices and then fail to do so, they may be liable for deceptive practices fraud and subject to action by the Federal Trade Commission).

Another approach can be found in the consultation papers of the Australian Government on the protection of privacy in the private sector[4], and notably in the information paper issued in September 1999.

Many factors, and most notably the privacy concerns that many people have in relation to electronic commerce, have influenced the Government's decision to develop a national legislative framework for privacy protection based on the *National Principles for the Fair Handling of Personal Information*

(National Principles) issued by the Privacy Commissioner (The federal *Privacy Act 1988* (Privacy Act) is the principal piece of legislation providing privacy protection in the federal public sector in Australia) in February 1998, following extensive consultation with business and consumers.

Briefly, the legislation will allow for the recognition of self-regulatory privacy codes backed by default legislative principles and a complaint handling regime that will apply where there is no applicable privacy code. The Privacy Commissioner will have a major role in the scheme. He or she will have an overall promotion and oversight role in relation to the private sector, whether covered by a code or not. The Privacy Commissioner will be responsible for approving privacy codes, providing assistance and advice to organisations, handling some complaints, and generally promoting an awareness and understanding of the scheme. As is currently the case in the Privacy Commissioner's limited private sector coverage, a determination of a complaint by the Privacy Commissioner or by a code complaint body will be enforceable in the Federal Court of Australia.

Another approach to be mentioned is the one adopted by Japan. In order to support personal data protection by business entities, the Ministry of International Trade and Industry (MITI) has issued model guidelines for business organisations entitled "Guidelines Concerning the Protection of Computer Processed Personal Data in the Private Sector (MITI Guidelines)". The Ministry of Posts and Telecommunications (MPT) has also issued guidelines for telecommunications services entitled "Guidelines on the Protection of Personal Data in Telecommunications Business (MPT Guidelines)". In addition, in March 1999, in order to encourage the appropriate management of personal data protection by each business entity, MITI established Japanese Industrial Standard (JIS) Q 15001 "Requirements for Compliance Program on Personal Information Protection". JIS Q 15001 requires the business entities to comply with the following:

- Establishment, implementation, maintenance and disclosure of a personal data protection policy.
- Limitation on collection of personal data.
- Limitation on use and disclosure of personal data.
- Receiving and responding appropriately to all complaints and requests for assistance from data subjects.
- Auditing; etc.

Further, JIPDEC (Japan Information Processing Development Center) grants "Privacy Marks" after certifying conformity of business entities to JIS Q15001 and MITI Guidelines. If the business entities granted "Privacy Marks" fail to conform to JIS Q 15001 and MITI Guidelines, JIPDEC should provide advice, request improvements, or may cancel the certification of Privacy Marks. Also, the "Personal Data Protection Registration Center", set up within the Japan Data Communications Association, registers telecommunication business entities which implement appropriate measures to protect privacy and issues a "personal data protection mark" to such businesses.

Conclusions on fundamental contract requirements

It is possible to summarise those elements which afford the core level of privacy protection to be reflected in the contractual provisions, as follows:

- Substantive rules based on the Principles in the OECD Privacy Guidelines. This element can be achieved through the inclusion of substantive principles into the contract or by reference to a relevant law, principles or guidelines.

- Some means of ensuring accountability and verifying that the parties are complying with their privacy obligations[5].

- A workable complaints and investigations process, in the event that there is a breach of the privacy obligations.

- Appropriate dispute resolution mechanisms for affected parties.

The particular circumstances of a data transfer may require more or less than the above-mentioned rules and procedure to be included in the contract. It may be that part of the required privacy protection is properly provided for by the wider legal or self-regulatory framework. Another consideration would be the nature of and risk attaching to the particular data which could either be non-sensitive public data requiring less protection or sensitive data requiring more protection.

3. CONTRACTUAL MODELS CURRENTLY IN USE OR UNDER DEVELOPMENT

Historic focus on business to business transfers

The idea of using contracts for TBDF has been around for some time. In the early 1990s, the prevalent form of TBDF involved business to business (B to B) transfers. The nature of these transfers is very wide-ranging. They include the supply or exchange of personal data between business units or divisions within the same organisation. B to B also contemplates one entity providing data processing services to another, and the transfer of personal data as either the subject of, or 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 direct marketing and travel reservations), and public sector agencies (law enforcement, border controls, tax agencies).

There has been a growing awareness of the significance of personal data as a key resource of many businesses. Although the impact of telecommunications on TBDF has long been well understood, the advent of the GII (in the form of the Internet and Intranet) has implications, which are only just beginning to be addressed. Global networks make it possible to collect, process and transmit personal data on an unprecedented scale. However, at the time contractual privacy solutions were first being debated, the focus was on more conventional B to B transfers, culminating in the development in 1992 of the Council of Europe Model Contract.

Council of Europe Model Contract (1992)

The Council of Europe Model Contract to Ensure Equivalent Data Protection in the Context of Transborder Data Flows was the result of a joint study by the Council of Europe, the Commission of the European Communities and the International Chamber of Commerce (ICC). The Model Contract is a collection of model clauses designed to ensure "equivalent protection", in the context of transborder data flows, based on the guarantees in Convention 108. As well as being applicable to the equivalent protection clause in the OECD Privacy Guidelines, the Council of Europe Model Contract provides a useful reference in determining what may amount to "adequate protection" under the EU Directive.

Under the Model Contract, the party sending the data warrants that the data have been obtained and handled in accordance with the domestic privacy laws of the country in which it operates. In particular, reference is made to fair and lawful data collection, the purpose for which the data have been stored, the adequacy and relevance of the data, the accuracy of the data and the period for which data storage has been authorised.

The party receiving the data undertakes to abide by the same principles that apply to the data exporter in its home country. To supplement this undertaking, the data receiver also agrees to use the data only for the purposes set out in the contract, to protect sensitive data in the manner required by the domestic law of the data sender, not to communicate the data to a third party unless specifically authorised in the contract and to rectify, delete and update the data as required by the data sender.

The remaining clauses deal with liability for the misuse of the data by the data receiver, rights of data subjects, dispute settlement and termination of the contract. The only detail on the mechanics of dispute resolution is in respect of arbitration (including the use of experts); the contractual requirement is for the parties to establish an "*appropriate system of settlement of disputes*".[6] The applicable law is left open as a matter for the parties to determine. This work of the Council of Europe (on contractual solutions) has provided a foundation for further developments.

The ICC Revised Model Contract

The 1992 Council of Europe Model Contract clauses were revised by the ICC, in light of the EU Directive's requirement of "adequate protection" in data exchanges to third countries. The revision takes into account the comments of the European Union's Article 29 Working Party set up pursuant to Article 29 of the EU Directive. The result was the ICC Model Clauses (For Use In Contracts Involving Transborder Data Flows).

The focus of the Model Clauses is on B to B transfers, whether off-line (that is by manual or physical means) or on-line (via electronic media). The latter medium is contemplated in the explanatory notes to the Model Clauses. They make another valid point; namely, the concepts embodied in the ICC Model Clauses should become acceptable to a broad spectrum of enterprises. As these forms and practices become more widely known within the general business community, they are more readily adopted and therefore the Model Clauses should be more widely applicable to a range of B to B transactions, including those entered into by small and medium-sized enterprises.[7]

There are certain assumptions within the ICC Model Clauses which may mean that some elements would require modification to tailor the use of the Model Clauses to the particular circumstances of the TBDF. For example, there are several references (in Clauses 2, 3 and 4) to the data importer constraining its subsequent use of the personal data to the purposes which have been notified by the data exporter or as is otherwise allowable under the laws of the country in which the data exporter is established. There is also a prohibition on disclosure (in the form of an onward transfer to a third party or country) without the prior consent of the data exporter.

The point is that these Clauses are a "model" and as such provide a strong basis on which to build or tailor certain clauses to reflect the particular requirements of the data importer/exporter and of the governing privacy laws or regime. If the Model Clauses are endorsed as satisfying the "adequacy" requirements of the EU Directive, then the parties modify those Clauses at their own risk; if the effect of any amendments is to reduce the level of privacy protection, then the parties could not make any assumptions that the arrangements reflected within the amended Model Clauses would be sufficient in terms of the requirements of the EU Directive.

Any detailed discussion of their content or consistency with the EU Directive is outside the scope of this report. However, the ICC Model Clauses have significant value as a foundation document or template for the development of B to B privacy contracts. The issue of individual redress in B to B contracts is discussed further in section 4.

Other work on contractual solutions

There have been a number of studies and initiatives in other fora on the use of model contracts for B to B data transfers. These include: the Working Document, adopted by the Article 29 Working Party on 22 April 1998, containing "Preliminary Views on the Use of Contractual Provisions in the Context of Transfers of Personal Data to Third Countries"; recommendations issued by the Office of the Privacy

Commissioner of Hong Kong in Fact Sheet No. 1, April 1997; work of the Information and Privacy Commissioner of Ontario, Canada; the UN/CEFACT LWG work on contractual models for electronic commerce (Trade/Cefact/1999/crp.5/Rev1); and the Privacy and American Business 1999 Model Contracts Project (P&AB). This Project is on-going and involves the development of a contract template for TBDF activities.

Experience with TBDF agreements

The ICC Model Clauses are being used within Europe primarily as a reference point for the development of ad hoc TBDF contracts and in the employment or human resources area. There have been other contractual privacy initiatives which have received considerable publicity as examples of high profile B to B privacy contracts.[8]

One such example is the agreement between German railways (Deutsche Bahn AG) and Citibank. In 1994, German Railways (Deutsche Bahn AG) arranged with the German subsidiary of Citibank for the production of railway cards (offering discounts for frequent travellers) which also functioned as VISA cards. Because the cards were produced by a Citibank subsidiary in the United States, the agreement gave rise to substantial transborder data flows. In response to German data protection concerns, an Agreement on Inter-territorial Data Protection was entered into to give German citizens the same level of privacy protection which they would have had if the cards had been produced in Germany. In particular, the contract provided for the application of German law, limited the transfer of the data to third parties, allowed for on-site audits by the German data protection authorities at Citibank's subsidiaries in the United States, and held German Railways and the German Citibank subsidiary liable to German data subjects for any violations of the Agreement by their American counterparts.

Although the experience with the Deutsche Bahn/Citibank Agreement is very instructive, its application as a precedent or model is quite limited because these types of contractual solutions may not be sufficiently "scaleable" or amenable to adaptation for smaller scale and lower profile B to B transfers.

Conclusions on current models

The international work on B to B contractual solutions is at a significant stage. There has been sufficient experience with these contracts for the development of a relatively detailed and comprehensive list of contractual requirements (in the form of the ICC Model Clauses). It is expected that there will be further advances on this work, as their uptake and adaptation increases. The expertise gained by those working with the ICC Model Clauses, and the need to tailor or modify their detail to adapt to particular circumstances, could be monitored and fed back into the "loop" for updating the ICC Model Clauses. It may be appropriate to develop variables or different versions to accommodate categories of industries/sectors or particular circumstances. No doubt this work will be further developed. It may also be enhanced by the experience gained from other ongoing projects.

The B to B contractual models are not that sensitive to, or dependent on, the medium of the transfer or communication. The ICC Model Clauses can be applied in the context of on-line (electronic) TBDF. The challenge, in terms of those contractual solutions which are currently in use or still under development, is that the focus has been on B to B; therefore, there has been little tangible progress on efficient contractual privacy solutions in C to B on-line TBDF. But the world is changing very quickly in respect of TBDF; there are now new pressures and issues to be addressed. The report will return to this theme in section 5.

4. RECOURSE OF THE INDIVIDUAL IN B TO B CONTRACTS

To date, the development of TBDF contracts has been predominantly to address B to B transfers (such as the ICC Model Clauses). There is a consensus from experience with B to B contracts that they have the potential to improve significantly the fair information-handling practices and to overcome the potential restriction on the transborder flow of data as a result of different approaches to privacy protection adopted by member state governments.

Individual redress

There are a number of issues affecting the recourse of the individual under B to B contracts. Individuals are reliant on data exporters effectively acting as their agents to secure the requisite privacy protection. The ICC model contract seeks to address these issues by giving the data subject or data protection authorities a right of action against the data exporter who can seek indemnification against the data importer. Lack of contract privacy, however, still remains a problem in the reducing number of jurisdictions which do not recognise third party rights under contracts. B to B contracts complemented by a legal or self-regulatory privacy protection infrastructure might provide an alternative solution to individual redress. The German Railways/Citibank is an example of this possibility.

Logistical and resource barriers

Other logistical and practical drawbacks with ad hoc B to B contractual solutions, such as the barrier of legal costs or the time and resources, can be overcome by model contracts.

Allocating risk and liability

On the issue of jurisdiction and choice of law, one theory is to structure the contract so that the exporter of the data undertakes under domestic law that the data protection practices will be followed by any importer of the data anywhere in the world. This is the approach underlying the ICC Model Clauses. The effect is that the exporter is liable for the foreign treatment of any exported data, and the data subject would be able to seek redress in his or her local jurisdiction against the exporter for the failure of the importer to comply with its privacy obligations.

Verification and certification

There may be a need for some type of verification or certification mechanism to confirm that the importer's data management or processing complies with the contractual privacy obligations. If the individual has easy recourse to an effective complaints-based privacy regime, then there is less need to emphasise verification measures.

The inspection and audit processes required by any verification measure have their origins in B to B contracts, but have been modified to suit the different characteristics of online C to B interactions focusing

on proposals to attach labels, seals of approval, privacy marks and otherwise to certify the privacy compliance of a Web site. Contracts could provide for verification if thought necessary by providing for audit inspection arrangements or transparency measures for the benefit of individuals. Verification can be resource intensive and the effectiveness of the measure is dependent on the choice of auditor.

The ICC Model Clauses contain an undertaking by the data importer to, "submit its data processing facilities, data files and documentation needed for processing to auditing and/or certification by the Data Exporter (or other duly qualified auditors of inspection authorities not reasonably objected to be the Data Importer and approved by the Data Exporter to ascertain compliance with the warranties and undertakings in these Clauses)" (see Clause 4).

Difficulty exercising individual rights

B to B contracts transferring personal data without the knowledge or consent of data subjects make it difficult for data subjects to "challenge data" relating to them. Although this does not negate the validity of using contractual solutions, it remains an outstanding issue.

What needs to be addressed is how the individual will know, or give consent to, the collection and transfer of her or his personal data (as required under the Collection Limitation Principle)? How will the contracting parties in a B to B transfer inform the individual of the purposes and uses for which personal data are transferred (per the OECD Purpose Specification Principle)? Will the individual be offered choice concerning or have the opportunity to consent to subsequent uses or disclosure of the data (per the Use Limitation Principle)? As mentioned above, a possible means of addressing these issues might be the solution adopted by the ICC Model Contract of giving the data subject rights of action against the data exporter.

The ICC model clauses solution

Applying the laws of the data exporter

The ICC Model Clauses address the issue of applicable law by requiring the data importer to comply either with data protection rules of the data exporter or a set of principles deemed to be adequate for data relating to citizens from the exporting country. This is consistent with the objective of the ICC Model Clauses: "to assist those who wish to transfer personal data from countries that regulate export of personal data to countries that do not provide protection for personal data that the source country finds adequate." A secondary benefit of the use of the ICC Model Clauses will be enhanced privacy protection for the personally identifiable information transferred pursuant to the contract where the receiving country does not provide effective privacy protection either through law or self-regulation."

The ICC Model Clauses require the data importer to permit the data subject the same rights she or he would have had against the data exporter in respect of the data prior to its export. This is a different issue from the data subject acquiring a directly enforceable right to sue under the B to B contract. The contractual position is that the data importer is assuming an obligation to ensure that the data subject can challenge the data (as this right is expressed in the applicable data protection law), such as by recognising any request for access to and the correction of his or her data.

Involvement of competent authorities

Another measure in the ICC Model Clauses is to incorporate the role of the data protection authorities or government supervisory agencies in redirecting complaints. The Clauses provide for undertakings by the data exporter to the effect that, "*the Data Exporter will promptly respond to inquiries from the Authority about the use of relevant personal data and to any Data Subjects' inquiry concerning use of her or his personal data, (including whether the same has been exported by it) and provide the inquirer with the name of the Data Importer and the individual responsible at the Data Importer who will be informed of the inquiry and who will respond to inquiries from its national authorities*"[9].

The effectiveness of this measure will be enhanced if the data subject is informed that her/his data are being processed and/or exported in the way contemplated by the B to B contract. Data protection rules will most likely require notice and choice. The effectiveness of this measure also depends on the ability of national data protection authorities to respond swiftly to inquiries made in the context of an ICC contract.

Involvement of the data subject

The dispute resolution provisions in the ICC Model Clauses expressly contemplate disputes involving the data subject. The data importer agrees to abide by the decision of the investigating data protection authority. A number of steps need to be taken before any dispute resolution process can commence; namely, notification and investigation of the data subject's complaint. The undertakings of the data importer include identification of an individual to deal with enquiries (and to notify the relevant authority) and to process complaints within the applicable timeframes of any data protection laws or self-regulation in the country of the data exporter.

Sanctions and remedies

"The ICC Model Clauses provide the data subject with the same rights as they would be entitled to in the country of the data exporter. The ICC Model Clauses also provide a right for the data exporter to terminate the agreement or to insist on the return or destruction of the data which is the cause of the data subject's complaint. One of the elements identified in the proposed common substantive reference for privacy clauses in a contract is the availability of remedies. Remedies for privacy breaches are a general issue that governments continue to grapple with and is not limited to contractual solutions. In the context of remedies for breach of contract, it is important to note that remedies vary from country to country. Examples of such remedies may include the following depending on the law of a member state: specific performance, recission, restitution, and damages. Specific performance requires the party in breach to perform his/her obligations under the contract. Recission is the cancellation of a contract and a return of the parties to their status prior to the contract. Restitution requires the party in breach to make the aggrieved party whole. In many countries, information is treated as an intangible to which it is very hard to assign a value. The significance is that, in a subsequent dispute the claimant may have difficulty quantifying their loss and proving that he or she has suffered loss or damage which has been caused by the breach of privacy obligations. It is important to note however that this difficulty is not unique to the contractual solution. Predetermined monetary compensation could constitute a remedy for breach of contractual obligations. Yet it may still be incumbent to demonstrate that the specified amount is based upon a genuine estimate of loss. This could be subject to challenge.

The need for directly enforceable rights under the contract

If the data protection authority or government supervisory agency cannot intervene to ensure the data subject obtains redress, the parties can discharge their obligations and take action against the other for any failure in this regard. This raises the issue of the data subject being able to sue the defaulting party under the B to B contract. In some jurisdictions, there may be an impediment in that the data subject is not a party to the contract (that is, there is no "privity of contract"). This impediment is being overcome as many countries have adopted laws which recognise the right of a third party, who is in receipt of a promise or other benefit under a contract, to enforce those particular obligations against the defaulting party.

This issue of the need for directly enforceable rights not only affects the data subject. If there is any onward transfer of the data by the importer to a third party, the exporter may have difficulty in ensuring privacy compliance. The exporter can impose contractual restrictions on the importer, to constrain subsequent processing and re-use (as is contemplated under the ICC Model Clauses). However, the exporter may have difficulties enforcing such restrictions, unless the law governing the contract allows the exporter (as a third party beneficiary to the primary contract between the importer and onwards transferee) to sue on that contract.

Informing the individual

Privacy notices and other awareness measures

The question of how the requirements of knowledge or consent of the data subject (such as under the OECD Privacy Guidelines) can be satisfied in the context of B to B contracts could be addressed by any ancillary measures which would not involve the design or content of the contract, but which would increase the awareness of data subjects as to the proposed uses of collected information.

If the requirements of the OECD Purpose Specification Principle are addressed by data exporters (or other collectors) at the time of collection, those data subjects will have a greater degree of knowledge and therefore empowerment, to exercise their rights in respect of a data challenge. This could also lay the groundwork for the data subject to take action against the data exporter for misrepresentation.

Contracting directly with the data subject

In the context of providing redress to a data subject, the European Union's Article 29 Working Party[10] has suggested a "tripartite" solution, where the data exporter enters into a separate contractual agreement with the data subject when collecting the data, stipulating that the exporter will remain liable for the consequences of any failure by the importer to comply with an agreed set of data protection principles. This could be used to overcome the problem of insufficient knowledge as well as any lack of privity of contract. The data subject would be granted redress against the exporter for the default or failure of the importer. It would be up to the exporter to recover any damages paid to the data subject by taking a separate action for breach of contract against the importer. Such a suggestion may be helpful in the few countries that do not recognise third party beneficiaries.

This tripartite approach would be feasible where the subsequent TBDF could be anticipated at the time of collection. There may be certain categories where the contract with the data subject would become part of standard terms and conditions on which certain organisations provide services. This would also be consistent with the OECD Openness principle and the need for transparency that aims to ensure the data subject is informed of his or her privacy rights. Nevertheless, these tripartite agreements might prove cumbersome and impractical.

Economies of scale

Where the amount of data to be transferred is minimal, it may not justify the use of a specific TBDF contract. There do not appear to be any cases, which have been widely reported, where ad hoc TBDF contracts have been used between a business and data subject on a one-to-one or one-to-many basis.

Conclusions on recourse of the individual

Concern has been expressed about whether business to business contracts can provide individual recourse. Although B to B contracts may not achieve redress for the data subject in all cases, various measures have been proposed in initiatives such as the ICC Model Clauses to address this issue. These proposals might well provide an adequate remedy in the majority of cases. The contractual approach illustrated by the ICC Model Clauses allows for the involvement of a data protection authority or government supervisory agency. Other contracts might provide for private sector dispute resolution.

There are a number of other issues with B to B contracts, involving jurisdiction and choice of law issues and the impact of the EU Directive, particularly the adequacy requirements. Although these matters are extremely complex, they have been addressed in the course of the development of template or model clauses.

In some respects, the seemingly more mundane and lower profile issues are, in practical terms, more problematic; in particular, issues such as unequal resources between the parties and the data subject, or the lack of information on the purposes of collection and the subsequent re-use of the collected information as required under the OECD Privacy Guidelines. In this regard, certain suggestions that arise in the context of C to B transfers could be equally applicable to B to B contracts; for example, the measures discussed in sections 5 and 6 to provide the data subject with access to rights-based information or education centres, greater reliance on an organisation's Privacy Statement, verification mechanisms, and recourse to a low cost, readily accessible dispute resolution process.

5. ISSUES WITH CONSUMER TO BUSINESS INTERACTIONS

The discussion in this section focuses on the characteristics of consumer to business data interactions in an online environment and the significance of these characteristics in terms of the ability to apply contractual solutions to C to B transfers on the Internet. It explores what mechanisms could be modified, or developed, to realise the aim of improved privacy practices in order to protect personal data collected via the World Wide Web.

Impact of the Internet on privacy

Until the emergence of the Internet, there was comparatively little direct contact between a consumer located in one jurisdiction and a business located in another. Individuals might purchase goods or services when abroad on holiday, but otherwise any international transactions would take place through an organisation with a physical establishment in the consumer's jurisdiction (for example, an airline or credit card company).

The growth in electronic commerce has transformed this situation, especially in relation to contracts for information products and services (such as books, music CDs, software and subscriptions) and increasingly also for other products available by electronic mail order. There is a burgeoning global marketplace. For consumers armed with credit cards and Internet access, the location of a supplier becomes irrelevant.

It is also the case that, historically, some of the most effective privacy protection derived from barriers of cost, distance, inaccessibility, incompatibility and undiscoverability. The capabilities of the Internet have transformed this situation. As stated before, online TBDF (from C to B) creates both new challenges and new opportunities for privacy protection. Online TBDF facilitates the collection of personally identifiable information that can be used to create a personal profile of a user, knowledge and consent regarding the collection and use of the personally identifiable data should be offered and the data subject's choice should be respected. In that respect, the deployment of technological solutions can facilitate consumer empowerment. Personal profiles could then be used to tailor and customise interactions between individuals and businesses.

Common issues between B to B and C to B

Many of the issues relevant to B to B contracts will also be relevant in a C to B context:

- Information to the data subject on the collection of data and the purpose for which it is collected.
- Enforcement of privacy breaches.
- Effective verification mechanisms.

Differences between B to B and C to B

Despite this, some significant differences exist between the two categories of TBDF relationships, which may require the adoption of other strategies. In B to B contracts, both parties will almost certainly be regarded as processing personal data to which the provisions of national laws or the principles in international instruments such as the OECD Privacy guidelines will be relevant. In many cases, the transfer of personal data will be the prime purpose of the agreement; for example, the sale of a list of names and addresses (increasingly e-mail addresses) which will be used for the purpose of direct marketing. In cases where the transfer is peripheral to the main purpose of the parties, for example the transfer of personal data concerning a passenger's itinerary between airlines within an international alliance, the transfer will take place in the context of an ongoing relationship between the parties.

The situation differs with C to B interactions. Often there will be no pre-existing relationship; the Web browsing may be random, with many first times or intermittent site visits. The exception is where the consumer has an established relationship, such as a history of ordering goods 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. 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" with personal data. 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.

As has already been mentioned, perhaps the most significant difference between B to B and C to B transactions is that the transfer of data will generally be initiated without a contract having been concluded between the participants. An example is where a business establishes a Web site from which it offers to supply goods or services. There is an analogy with a traditional shop. At the stage the consumer enters the shop, there is no existing contract with the storekeeper. Similarly, the act of accessing a Web site will not of itself suffice to establish a contractual relationship between the site owner and visitor. This is despite the fact that, where a Web site uses devices such as cookies to derive and match information to an identifiable individual, personal data may be collected from the moment the user accesses the site. As will be discussed further, this characteristic of online C to B interactions requires that any attempt to protect the privacy interests of the consumer begin prior to the contractual stage.

Need for a range of privacy measures to address C to B

If the characteristics of a C to B transfer are considered in light of the common substantive reference (discussed above), it may still be possible to address the privacy protection requirements, even though there may be difficulties in fitting the C to B interaction within a contract structure. It would require other ways to encourage businesses (data importers) to adopt privacy protection measures. There are obvious impediments in giving effect to a national data protection law in a networked environment where there is no geographical proximity of the various participants in an online TBDF and where territorial boundaries have been rendered irrelevant. There are constraints on the extent to which any national data protection law can have extra-territorial effect. Therefore, effective private or self-regulatory measures are an important means of achieving the aims of the OECD Privacy Guidelines.

With regard to the feasibility of a global privacy standard, an ad hoc advisory group on privacy undertook a study on behalf of the International Standards Organisation (ISO) to examine whether there is a need for an international standard to address information privacy, measure privacy protection and ensure global harmonisation. The advisory group concluded that it was premature to reach a determination on the desirability and practicality of ISO undertaking the development of international standards relevant to the protection of personal data.

Importance of model privacy protection policies

In the context of C to B transfers, there may be an important role for educational measures to assist organisations in developing accurate privacy statements. An example is the privacy statement generated by the use of the Privacy Policy Statement Generator developed by the OECD (the tool is referred to as the "Generator" and its output as a "Statement"). The widespread practice of developing a formal privacy policy for a business (supplier/data importer), and then reflecting that policy in a statement such as the one produced with the help of the Generator, could have a cumulative but significant effect on the general level of awareness of consumers about the information-handling practices of the Web sites and businesses with whom they interact on the Web.

Certification measures for online transfers

Another consequence of the growth in global C to B transfers is the interest in developing verification tools or measures which would be suited to the online environment of the World Wide Web. In a global marketplace, where there is no direct or physical relationship between the parties to an interaction over the Web, issues of consumer trust and confidence become critically important. For this reason, the efforts to develop certification measures (including the use of privacy marks, labels and seals), can be seen as a proactive measure undertaken by the private sector to ensure consumer trust and confidence. This situation can be contrasted with those other privacy measures, which assume a complaints-based regime and place greater reliance on the ability of individuals to enforce and obtain redress in respect of the privacy obligations. The interest in verification measures is a realistic recognition of the logistical and legal barriers facing data subjects (consumers) in C to B transborder data flows.

Individual redress and enforcement

This line of discussion inevitably leads to the difficulties of pursuing individual redress and enforcement and to the need for dispute resolution options which are tailored to the particular characteristics and needs of C to B transfers. This is a conclusion, and area of interest, shared by other organisations who are currently addressing the implications of the GII, whether on the issue of dispute resolution mechanisms for electronic commerce transactions or to resolve complaints over domain name allocation. The significance of the issue of dispute resolution, and the availability of certain options, are discussed in section 6.

Benefits for business

The development of C to B privacy measures, such as Privacy Statements, might be seen primarily as benefiting the consumer. The approach may also assist businesses, especially small and medium-sized enterprises. Where suppliers lack a background in international trade, they may well be unaware of the legal requirements applying in other jurisdictions relating to matters such as data protection and direct marketing. The possibility of adopting model terms and policies may be of considerable benefit in limiting exposure to customer complaints (and even litigation) and to building consumer trust and confidence,

which is a pre-requisite to successful competition in electronic commerce. However, a posted privacy statement can create legal liability for a business if it is not accurate. Therefore, any model policy or statement must be carefully reviewed by a business to ensure that it is consistent with the business' information practices and compliant with applicable regulation.

Issues with applying a contractual analysis to C to B

There are various legal requirements for the formation and content of an enforceable contract, and there are significant differences between national laws (on contracts). However, the following analysis aims to identify a number of common elements which, when applied in the context of contractual privacy solutions, pose difficulties for C to B transfers. A significant number of C to B interactions cannot be analysed in contractual terms. They either do not contain the elements of a contract or do not satisfy the pre-conditions to create a contract.

Requirements for the formation of a contract

In general, the doctrine of freedom of contract permits parties to contract in such manner and subject to such terms, as they think fit. Requirements that contracts be attested by the signatures of the parties, or otherwise concluded in writing, have been identified as impediments to the expansion of electronic commerce. Various proposals have been put forward to address these, such as by recognising the legal validity of electronic or digital signatures. These matters are outside the scope of this report.

The key requirement for the formation of a contract is that there should be an intention to creating a binding obligation, as evidenced by an offer from one party, which is accepted by the other. Where contracts are concluded at a distance, it may be important to determine at what point in time or in the ordering process, agreement is reached; that is, when does the contract become irrevocable? Once agreement is reached, neither party can unilaterally modify its terms although the original contract could provide for modification on notice from the business. Those pre-requisites may be of considerable importance in relation to data protection issues. If a consumer has not been informed of, nor agreed to, the supplier's intentions regarding the subsequent processing of personal data at the time the contract is concluded, is there still a binding contract in respect of the subsequent use of those data? On what basis can it be argued that the supplier (business) is constrained by the previous dealings or undertakings to protect the consumer's privacy?

In many legal jurisdictions, for a contract to be binding requires that there should be an offer from one party which is accepted by the other. It will be important to identify when these stages are reached. In general, when a supplier indicates that goods or services are available for supply, this does not of itself constitute an offer; rather the common law courts have treated this as an invitation to the consumer to make an offer. This offer may then be accepted by the supplier. The contract is formed. The exact timing of the formation will be dependent on the applicable rules of acceptance.

The rules of acceptance are now under review within those countries that are seeking to modernise their laws and provide greater certainty as to their application in an online environment. To illustrate, the EU Directive on Electronic Commerce acknowledges that a supplier may be treated as making the offer, but provides that:

> *"Member States shall lay down in their legislation that, save where otherwise agreed by professional persons, in cases where a recipient, in accepting a service provider's offer, is required to give his consent through technological means such as clicking on an icon, the*

> *contract is concluded when the recipient of the service has received from the service provider electronically, an acknowledgement of the recipient's acceptance." (Article 11)*

The acknowledgement, which must be sent immediately, will be deemed to have been received when it becomes accessible to the consumer. This is not necessarily the same as having been seen by the consumer. Delivery of the acknowledgement into the consumer's electronic mailbox may suffice. This is another contract element which is currently under scrutiny.

Work is also being conducted by the International Chamber of Commerce (ICC) on the proposed establishment of Uniform Rules on Electronic Trade Settlement. These adopt a different approach by providing that:

> *"An electronic offer and/or acceptance becomes effective when it enters the information system of the recipient in a form capable of being processed by that system." (Rule 2.1)*

In the United States, the Uniform Computer Information Transactions Act provides that:

"SECTION 203. OFFER AND ACCEPTANCE IN GENERAL. Unless otherwise unambiguously indicated by the language or the circumstances:

(1) An offer to make a contract invites acceptance in any manner and by any medium reasonable under the circumstances.

(2) An order or other offer to acquire a copy for prompt or current delivery invites acceptance by either a prompt promise to ship or a prompt or current shipment of a conforming or non-conforming copy. However, a shipment of non-conforming copies is not an acceptance if the licensor reasonably notifies the licensee that the shipment is offered only as an accommodation to the licensee.

(3) If the beginning of a requested performance is a reasonable mode of acceptance, an offeror that is not notified of acceptance within a reasonable time may treat the offer as having lapsed before acceptance.

(4) If an offer in an electronic message evokes an electronic message in response, a contract is formed:

(A) when an electronic acceptance is received; or

(B) if the response consists of beginning performance, full performance, or giving access to information, when the performance is received or the access is enabled and necessary access materials are received."

Other circumstances influence the contractual analysis for TBDF. A complicating factor in many cases will be the consumer's use of a credit card to finance the transaction and the need to supply these details in advance. The card details may well be processed and verified by the supplier before the consumer is informed that the order has been accepted. Where the supplier has effectively accepted the consumer's money, it may be difficult to argue that a contract has not been concluded.

If Privacy Statements are to be incorporated in C to B contracts, it should be clear which version of a statement applies to any particular contract. Technical or procedural arrangements should be developed to ensure certainty in consumer contracts based on the content of Web pages and similar global network documents.

Reconciling the different approaches to online contracts

These examples demonstrate that the pre-requisites for contract formation in an online electronic environment are not yet settled. There is a range of approaches currently being advocated and considerable international effort is being spent to produce a harmonised approach to online contracts. This has significant implications for applying contract structures to C to B interactions on the Web. When a consumer visits a Web site, the browsing activity can generate data . This is a form of data transfer; it could well 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 the contractual requirements of an intention to be bound, or offer and acceptance analysis, would apply to what is in essence only a communication or interaction.

For those C to B 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 C to B 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.

Use of the Internet to record contract formation

The information storage and recording capabilities of the Internet may also provide an opportunity. Unlike the vast majority of 'real life' contracts which may be entered into on an informal basis, with little if any recorded evidence of the fact of agreement and still less of the terms which have been negotiated, the use of the Internet provides the opportunity for the maintenance of a complete record of every act which took place during the formation and conclusion of a contract. The fact those data are recorded may be a privacy concern in its own right, but the existence of a record could assist in reconstructing all aspects of the contract formation process should this become necessary.

The potential of privacy policies and statements in C to B transfers

Privacy policies and statements are a means of giving notice to individuals. Such notices are capable of giving rise to both contractual and other legal obligations such as statutory or regulatory liabilities. Those obligations can be enforced depending on the nature of the liability and the rules of the particular jurisdiction - by contractual parties, individual data subjects, or public bodies.

The need for early warning on privacy

In order to afford the consumer genuine freedom of choice as to the transfer of data, notification of the uses to which personal data may be put should not only take place at the stage when a contract for the supply of goods or services is concluded, but privacy protection issues should also be brought to the consumer's attention at the earliest possible stage in the Web site interaction.

It would be quite possible for a site to adopt and publicise a privacy protection policy. This would inform the consumer of the nature of the data, which will be collected from the Web site visit, and the subsequent uses to which it may be put.

Enforcing a Privacy Statement

Privacy protection provisions incorporated into a C to B contract would entitle the consumer to take action to enforce these. But in some jurisdictions the legal status of privacy protection policies or statements may not be clear and there may be limited prospect of enforcement by an individual consumer. Either way, practical impediments should be overcome by any individual consumer who would attempt to issue proceedings against a business which is operating on the Web, given the amount of resources 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. These are all reasons for designing dispute resolution mechanisms which would permit ready access by consumers and businesses alike, and which would gain widespread credibility and acceptance among business. The effort should be on designing online complaints and dispute resolution processes where the benefits of implementing and upholding those processes are self-evident to the businesses, Web site designers and Internet Service Providers who have control over online data transfers.

In the United States, the Federal Trade Commission (FTC) is authorised, under Section 5 of the FTC Act that prohibits unfair or deceptive acts or practices, to take action against organisations that engage in unfair and deceptive acts or practices in or affecting commerce. The FTC has stated that it is a deceptive practice to misrepresent in a material fashion the purpose for which information is being collected from consumers and how the information will be used. Such acts or practices could include misrepresentations by organisations that they adhere to their posted privacy statements, when, in fact, they do not.

The evidentiary, security and authentication requirements of a binding privacy contract would be no different from the issues in electronic commerce B to B contracts. The resolution of these issues (in the electronic commerce context) would need to be applied to C to B privacy contracts.

The need for verification mechanisms

The issue of verification, whether in the form of self-assessment, certification, labelling or otherwise, may be of considerable significance in the area of consumer to business transactions. The consumer must have faith in the information practices of a remote Web site, whose location is unknown and the identity of the persons or businesses responsible may prove to be untraceable. As there is limited prospect of negotiation between consumers and businesses regarding the terms of contracts, some form of third party involvement may be desirable to provide a form of approval that the contract satisfies the requisite standards or expectations for privacy protection and that the site or business is complying with its privacy obligations. A similar suggestion can be made with respect to privacy policy statements.

Options for online verification

The need for some form of verification mechanism has already been addressed in the discussion on B to B contracts. The ICC Model Clauses contemplate a range of options involving third party inspection or audit of the data importer's compliance with its privacy obligations. In the context of C to B transactions, this issue has been seen more as a consumer protection concern. The characteristics of the online environment, where the data are most likely collected via a Web site, has focused attention on the use of privacy marks, labels and seals as a form of certification, rather than the act of physical inspection or audit which presupposes physical proximity. There have been numerous international initiatives to develop verification measures for use on the Internet. Some of these are canvassed below.

The Better Business Bureau Online Privacy Seal, the TRUSTe Web site and the Japanese Mark systems on privacy protection, aim to offer new options to enhance privacy in an online environment. They could also be applied to the trans-national processing of personal data. Web sites always generate transborder data flows and therefore the US Web sites that are licensees of BBB Online and TRUSTe seal are in fact attempts to support privacy protection in a global online environment. They rest on self-regulatory schemes initiated by US private industry.

The Japanese Mark Systems on privacy protection are the Japanese Privacy Protection Mark System and the Granting Mark System. Since April l998, the Japan Information Processing Development Centre (JIPDEC) operates the former and the latter is operated by the Japan Data Communications Association. JIPDEC grants Privacy Marks after a process of certification in which the handling of personal data in compliance with MITI (Ministry of International Trade and Industry) Guidelines of l997 is monitored. The Japan Data Communications Association also grants the marks for telecommunication carriers and service providers, after assessing compliance with the MPT (Ministry of Posts and Telecommunications) Guidelines of l996 and l998.

Role of privacy enhancing technologies

The World Wide Web Consortium (W3C) has launched the Platform for Privacy Preferences Project (P3P). This is intended to support a contractual agreement between information providers and users on the World Wide Web to allow in a flexible manner for the user's privacy preferences to be taken into account by the provider. Leading software manufacturers have announced that they will incorporate P3P into their latest versions once it is agreed by the W3C.

P3P relies on a number of technical conditions, which may not yet be in place. The browser software at the user end as well as the provider end will have to be compatible to allow for the necessary negotiation process between the PCs and servers. Different preferences may prevail in different parts of the world, (for example, in the EU and the US as opposed to Arab or Asian countries) raising compatibility issues.

Another example, which might be considered as the basis for action, is the Microsoft Merchant Server used to set up an electronic commerce operation. A wide range of retailers makes use of the software. The advantage of such a standardised set up is that there is an opportunity to build privacy policies into the design of the software. At present, however, it appears that privacy protection is addressed only in relation to the inclusion of encryption packages to enhance security for the exchange of financial data. Further consideration could be given to the possibility of working with major software developers and suppliers to ensure that the need for privacy protection is taken into account through all stages of the design, production and use.

Consumer protection initiatives

There are a number of parties, whether governmental or non-governmental, which could play a role in online user consumer protection including privacy. Examples might be Better Business Bureaux in the United States, which are charged to protect the interests of consumers.

The Better Business Bureau Online (BBB Online), TRUSTe, and WebTrust have formed and developed third party enforcement regimes that promote compliance with information practice codes. These enforcement regimes include the display of a seal or trust mark to notify consumers that Websites follow fair information practices. All of these organisations provide dispute resolution mechanisms, monitor compliance, and impose consequences for non-compliance (sanctions or expulsion from the seal program).

Companies that violate their stated information practices are also subject to FTC enforcement under Section 5 of the FTC Act.

Such bodies may well have an input into discussions although in some cases the associations are themselves active in commercial matters. In the United Kingdom, for example, the Consumers' Association sells books and magazines, provides its own credit card and operates as an ISP.

In some cases (for example, the Web Trader Scheme operated by the United Kingdom's Consumers' Association), accredited business is allowed to use an appropriate label on their Web sites. Businesses are required to undertake to observe a code of practice, which includes an obligation to conduct business in accordance with the terms of the Data Protection Act 1998. The Consumers' Association guarantees to make good up to GBP 50 of financial loss resulting from misuse of credit card details transmitted to an accredited trader. No liability is assumed for other losses including those resulting from breach of the Data Protection Act.

The existence of an umbrella organisation for businesses might offer potential for incorporating privacy terms and conditions as a pre-condition to obtaining admission to a Web site. An example of such an organisation is Bizrate. Located in Los Angeles, this operates a Web site containing listings of businesses in a wide range of categories. The condition attached to listing is that the business should accept assessment either by the organisation's staff or by its customers. In both cases, assessment is conducted on the basis of a wide range of features including the posted privacy policies. There may well be a valuable role for certification and labelling schemes to support other privacy measures, such as the use of Privacy Statements. Where the consumer and business are located in different countries, it may prove extremely difficult for the consumer to enforce any rights against the business. If alternative dispute resolution facilities were to be built into these schemes, this might provide a valuable addition to the consumer's legal rights, as discussed in the following section.

Enforcing the privacy commitment in C to B

The privacy rights of a consumer may be found in national laws and may be exercised in the prescribed manner. Most data protection regimes recognise electronic media and data so that if the online activity falls within the local jurisdiction, the consumer should have redress to the competent authority.

Reliance on contractual rights

Where a business indicates its adherence to a privacy protection policy, it is likely that compliance will be regarded as a term of any contract with the consumer. The C to B contract has an advantage over B to B, in that the data subject in a C to B transfer is most likely a party to the contract; and therefore the issue of lack of privity of contract would not be relevant. If a breach occurs, there may be a range of available legal remedies although in the environment of the Internet their efficacy may be questionable. In theory, any breach by the business of a contractual undertaking not to disclose personal data to third parties would be actionable by the consumer. Even though an action might be brought to interdict the business against further breaches, it would not undo the data transfer, and the consumer's redress might suffer from the same limitations as have been discussed under B to B court actions.

In cases where there is no contractual relationship between the consumer and the business (for example, the consumer's details have been recorded when visiting the site but no contract has resulted), it may be that the business would be in breach of its contractual obligations to any third party which has certified the acceptability of the business's privacy policies or which has permitted the use of a commendatory label. Historically, such situations have prompted concerns from common law countries, on the basis that

contractual rights and remedies belong only to contracting parties, but as noted earlier, the contracts privity issue has been resolved by many countries enacting specific legislation to recognise third party beneficiary rights. There remains, of course, the query of how effective any available remedy might prove.

Availability of other civil remedies

The range of civil remedies available to a data subject is not limited to those found in privacy legislation. There may be a range of other applicable consumer protection laws. Typically, these prohibit unfair or misleading advertising, (see the OECD Inventory of Instruments and Mechanisms Contributing to the Implementation and Enforcement of the OECD Guidelines in Global Networks). The general laws relating to breach of contract, fraud and fair trading may also apply where the data controller has violated the terms of a privacy statement, an online agreement (such as the terms and conditions associated with a registration form) or a transborder data flow contract. Such a breach may give rise to a number of possible civil remedies. Essentially, by providing notification of its privacy practices, a Web site represents or offers a commitment that it will follow these practices. Depending on the nature of the breach, most jurisdictions provide consumer protection and trade practices remedies for wrongful misrepresentations and/or fraudulent conduct if that commitment is broken.

Determining which law and jurisdiction should apply

Defining territoriality by geography

In a C to B transfer there can be many participants (or "actors"). It is quite simplistic to talk in terms of consumer to business. 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 of these actors (including data controllers) and activities may be "located" in different legal jurisdictions. It will probably be the norm rather than the exception that the participants in a C to B transfer are unknown to each other (rather than being seen as senders and recipients in a pre-determined relationship). 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? 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.

Choice of law and jurisdiction

The choice of law (jurisdiction to prescribe) will be highly significant in the adaptation and uptake of contractual privacy solutions. 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). Despite 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 when and where a contract is concluded is a major factor in determining which legal system is to govern the particular transaction. As discussed, 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 of 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 for example that the contract should be governed by Canadian law but that any disputes should be brought before the German courts.

Consumers' rights

Within Europe, the Brussels and Rome Conventions[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 OECD has pointed out, in the context of tax harmonisation, that the notion of permanent establishment, which is of major importance in determining whether an undertaking is liable to national taxes, may not be appropriate for electronic commerce.

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.

In the United States, generally jurisdiction can be established based on a three-prong test: 1. purposeful availment of the privilege of doing business in the forum state; 2. the cause of action must arise from the defendant's activities with respect to the forum state; and 3. there must be a substantial enough nexus between the defendant's acts and the forum state to make the exercise of jurisdiction reasonable.

Developments in electronic commerce

More recent developments may complicate matters. The European Union has recently published a Directive in the field of Electronic Commerce. This provides that, albeit within the European Union, transactions entered into by electronic means should be regulated by the law of the supplier. This approach is justified on the basis of supporting the development of the e-commerce new industry. At the same time, however, the Commission is proposing amendments to the Brussels and Rome Conventions, which would have the effect of subjecting all consumer contracts to the law of the consumer's domicile.

Some believe that there is an inescapable tension between choice of law and jurisdiction provisions designed either to provide a predictable environment for suppliers or, on the other hand, to assist consumers in pursuing their remedies. Online alternative dispute resolution (ADR) may be the most effective means of overcoming this issue. In this regard, the 1999 OECD Guidelines for Consumer Protection in the Context of Electronic Commerce recommend the use and development of ADR

mechanisms to address consumer complaints and to resolve consumer disputes arising from business to consumer electronic commerce, with special attention to cross-border transactions. 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 of how much autonomy should the contracting parties have to determine their choice of law and jurisdiction will therefore be a key one.

Conclusions on C to B transfers

There is a need to take steps to protect consumer privacy on the Internet based on the OECD Privacy Guidelines. There is no single solution for the regulation of C to B data transfer. There are mechanisms to assist consumers in making informed choices about the collection and use of personally identifiable data prior to the conclusion of a contract.

Privacy protection policies, resulting in a posted statement, have a significant role to play. Tools such as the OECD Generator may assist companies in developing a privacy statement that may be a binding commitment. A significant role can be identified for consumer protection agencies and third party organisations to provide certification or verification services and tools; perhaps even to oversee the implementation and maintenance of policies by those businesses who have either committed to such an arrangement, or who are members of an industry or association and subject to a governing body or code of practice.

In many cases, in the context of C to B transfers, the focus would stay on preventive and educational measures such as privacy statements and verification. Even if the privacy statements prove ineffectual in terms of their contractual force, there would still be benefit to be derived from this measure because of the role of privacy policies in creating data subject and data controller awareness.

Education should not, however, be the only focus. Work may also be done on the benefits of prescribing in advance the applicable dispute resolution options. It may be possible to adapt the existing online dispute resolution projects to provide a tailored service capable of providing a 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.

6. THE NEED FOR APPROPRIATE DISPUTE RESOLUTION MECHANISMS

The availability of dispute resolution mechanisms to resolve disputes between data controllers (businesses) and data subjects (consumers) over TBDF, has been identified as a fundamental requirement by several Member governments. There is a range of conventional and alternative dispute resolution mechanisms, which are described in this section. The discussion includes the advantages and disadvantages of each mechanism in respect of the specifics of the online environment that some observers have identified; a description of some of the international developments on online dispute resolution; and projects of interest to establishing mechanisms. Some possible suggestions for developing C to B online privacy dispute resolution mechanisms are provided as food for thought in the final part of this section.

Range of available dispute mechanisms

A critical consideration is what recourse the parties will have if a dispute arises. The following is a general discussion of the advantages and disadvantages of the various options, and of enforcement issues. The discussions on alternative dispute resolution (ADR) for the online environment are at a very preliminary point. In discussing options to address C to B disputes, the features of the dispute resolution mechanism are important. This discussion is to help to begin to identify key elements to be addressed for developing online mechanisms to resolve transborder C to B disputes.

Litigation

Litigation is always an option, but primarily in the B to B situation. The parties can agree that any dispute that may arise will be governed by the substantive law of a particular jurisdiction and submitted to the courts of a particular jurisdiction. Alternatively, if the parties have made no advance agreement, one party can, after a dispute has arisen, file a lawsuit in a particular jurisdiction. The parties could choose the forum where the contract was entered into, the forum where the contract was to be performed, or some other forum with a connection to the subject matter of the contract. In a B to B transaction there is a greater likelihood that such an agreement might be upheld by the relevant courts.

The situation changes, however, in a C to B transaction. The business entity may have a standard dispute resolution clause, which provides that any disputes must be resolved in the forum of the business entity. However, many jurisdictions are reluctant to impose a choice of jurisdiction provision against a consumer with less bargaining power. Many courts have invalidated a choice of forum selection, which compels a consumer to litigate in the forum of the business entity. There is therefore no guarantee that the courts of a given jurisdiction will uphold such a provision.

Advantages of litigation

A party may have the advantage of knowing that any dispute will be resolved in a forum with which it is familiar, and that the procedural and substantive law, which will be applied is one with which it has had

experience. Unless the parties see a particular advantage to a particular forum, generally, only a party with a stronger bargaining position will be able to secure such an advance agreement.

The court will render a decision, which will set a precedent. To clarify a matter of law, it may be advantageous to proceed to litigation in order to have a final ruling on the matter. Other forms of dispute resolution generally do not provide the parties with a result that can set a precedent. Furthermore, litigation results in a final decision by a court, which the winning party will seek to enforce against the losing party. In most jurisdictions, the losing party has the right to appeal against an unfavourable decision. This right of appeal is not typically available in most other forms of dispute resolution

Disadvantages of litigation

There are also disadvantages. First, litigation can be lengthy: perhaps a period of years. In addition, litigation can be extremely costly. Furthermore, a losing party frequently has the right to appeal, thereby increasing both the cost and the length of the procedure. In most venues, litigation is not a confidential proceeding. Where a case is particularly sensitive, the public nature of litigation can be a deterrent. In addition, in cross border situations the winning party may still have to go to the losing party's jurisdiction to enforce the judgement.

Alternative dispute resolution

Parties to cross-border contracts can agree to submit disputes to alternative dispute resolution. The ADR mechanisms can be tailored to offer the parties maximum flexibility. Many ADR processes are consensual, rather than adjudicative. ADR combats certain disadvantages of litigation and arbitration, by being cheaper, faster, and broader in outlook and by allowing the parties more control over the process and the outcome. Below are presented some of the ADR options.

Arbitration

As with litigation, arbitration results in a binding decision, which can be enforced against the other party. In ad hoc arbitration the parties agree to arbitrate but do not choose one of the many arbitral institutions to administer the arbitration. While ad hoc arbitration may be less expensive than institutional arbitration, the parties will have to take on the organisational tasks normally carried out by the staff of the various institutional entities.

In "institutional" arbitration, the parties submit their dispute to one of the many recognised arbitral institutions, such as the International Chamber of Commerce ("ICC"), the American Arbitration Association ("AAA"), the World Intellectual Property Organisation ("WIPO") or the London Court of International Arbitration ("LCIA"). The parties can agree in their initial contract to submit any disputes to arbitration, or they can agree to do so after a particular dispute has arisen. If the parties agree to submit their dispute to institutional arbitration, they must follow the rules and procedures set forth by the respective institutions. Unless the parties have agreed, they are not bound by judicial rules of procedure and evidence, and frequently have more flexibility than they would in a court proceeding.

Advantages of arbitration

Arbitration has certain advantages: the parties are free to choose their respective arbitrators and the applicable law and procedure which will govern the arbitration; a party can chose an arbitrator with a

particular expertise in a given field, and the parties can avoid litigating in the courts of their adversary. Generally, arbitration is less costly and faster than traditional litigation. The parties can provide for shortened time frames, which can speed up the arbitration and lower the cost.[12]

Arbitral awards are enforceable under the New York Convention on the Enforcement of Foreign Arbitral Awards.[13] Over 100 countries are signatories to this Convention. It requires the enforcement of a foreign arbitral award with limited exceptions. Enforcement of an arbitral award is frequently less complicated and costly than the enforcement of a foreign judgement, where one country may not necessarily recognise or allow for enforcement of a court judgement from a foreign jurisdiction.

Finally, with some exceptions[14], arbitration is not a matter of public record, as with most litigation. The conduct of the proceedings and the decisions are typically not available to the public. This can be a significant advantage.

Disadvantages of arbitration

Arbitration is consensual. If a party does not consent to arbitration, it cannot be forced to. Arbitration can be time-consuming and expensive, and arbitral awards do not set a precedent, so the parties may end up arbitrating the same issue more than once with different parties.

Complex matters frequently arise where the rights of third parties must be adjudicated in order for a dispute to be finally resolved. Without the third party's consent to arbitration, the arbitral panel has no authority to make a decision binding the third party, and the proper recourse would be to litigation, assuming the courts had jurisdiction over the third party. So in a B to B contract where the issue in dispute was the rights of a third party (such as a data subject), arbitration may not be a practical method of dispute resolution.

Mediation

Mediation involves a structured procedure, facilitated by an independent third party. The authority of the mediator is consensual. The mediator assists the parties to the dispute to recognise each other's interests and to identify options for resolution, but has no power to give a view on an outcome or to impose a decision. Many organisations assist parties seeking to mediate. Typically, a party can withdraw from mediation at any time.

Advantages of mediation

Mediation provides a less formal but disciplined method for the resolution of disputes. The parties are free to select a mediator knowledgeable in a particular field and to agree the applicable law or self-regulatory principles or code of conduct that will govern the mediation, with more latitude than parties involved in traditional litigation. Procedural flexibility permits the parties to reach creative and innovative solutions to their disputes.

In a mediation, the parties are free, if they choose, to introduce any piece of evidence or information which might assist in the settlement of their dispute, and they can often reach agreement faster and at less cost than in a more traditional dispute resolution forum. Mediation is generally less adversarial and can be an ideal method of settling a dispute where the parties wish to continue in their relationship.

Disadvantages of mediation

The procedure, if successful, results in a settlement. Many courts will enforce those agreements. However, in other jurisdictions, courts will not enforce mediation agreements.

Mediation does not necessarily result in an agreement. The parties can agree to mediate but if unsuccessful in reaching an agreement, they would have to resort to another form of dispute resolution, such as litigation or arbitration.[15]

It is also possible for mediation to achieve widely disparate results, even in substantively similar disputes.

Mediation-arbitration ("med/arb")

In "med/arb" procedure, the parties provide that in the event of a dispute they will attempt to resolve the dispute by mediation but, if the mediation is unsuccessful, the parties will agree to submit the dispute to arbitration.

This has the advantage of significant cost and time savings if the parties are successful in reaching a solution via mediation, but still preserves the parties' right to seek an arbitral award if the mediation is unsuccessful. Generally med/arb is most successful when the parties put a time limit on how long they are willing to mediate before resorting to arbitration.

Mini-trials and expert determinations

Two other forms of ADR, are mini-trials and expert determination. A mini-trial is a procedure where the parties meet in the presence of a "Neutral" and, after hearing presentations on the merits, the Neutral gives an opinion on how a court would be likely to rule, hopefully facilitating a voluntary settlement between the parties. Under expert determination or evaluation, the parties agree to submit certain key issues to an expert for determination. The parties can then incorporate the expert's findings into either a subsequent process or into a binding agreement.[16] These two methods have the advantage of speed and cost-efficiency. They are voluntary and the outcome is non-binding unless the parties agree to incorporate the expert's findings into a binding agreement.

Enforcement mechanisms

Conventional enforcement mechanisms

Even if litigation may be the last resort option, there is still the issue of the enforcement of any judgement. Notwithstanding international agreements such as the Brussels Convention and domestic rules such as the US requirement to give "full faith and credit" to judgements of other states, the problem of enforcing a foreign judgement remains.

The enforcement of foreign arbitral awards is governed by the New York Convention, which strictly limits the grounds for non-enforcement of an award. Therefore, a party who obtains an arbitral award is likely to be able to enforce it as long as the enforcement country is a signatory to the Convention.

Online enforcement mechanisms

Various online dispute resolution mechanisms have been created in the last few years, a number of which are described below. Enforcement is being addressed by some of these projects providing an escalation process. For example, BBBonline provides for a third party arbitration/mediation programme if a dispute cannot be resolved with the Subscriber Company.

Examples of online dispute resolution mechanisms

TRUSTe

TRUSTe[17] is a well-known initiative under which consumers can resolve issues relating to their individual privacy rights (TRUSTe) and other consumer issues. Web site owners sign a one-year contract with TRUSTe, which binds the user to certain privacy principles, and provides for escalation procedures in the event a dispute cannot be resolved. TRUSTe reviews the Web site, to ensure that it complies with the TRUSTe privacy principles. There is a dispute resolution mechanism, which provides for TRUSTe's review and escalation of the dispute resolution process if necessary.

BBBonline

Similarly, BBBonline[18] was established to help foster consumer trust and confidence in e-commerce. The BBBonline Privacy program offers a comprehensive assessment process to measure a company's ability to stand behind the promises it has made in its online privacy statement, and provides for a dispute resolution process in the event a consumer has a concern over a privacy issue.

WIPO

The WIPO Arbitration and Mediation Center provides dispute resolution services for challenges related to abusive registration and use of Internet domain names, commonly known as "cybersquatting", on the basis of the Uniform Domain Name Dispute Resolution Policy adopted by the Internet Corporation for Assigned Names and Numbers (ICANN). The Procedure is largely conducted online[19], with online direct submission of complaints also being available. Cases are decided over an average period of 45 days against a basic fee of USD 1 500.

CRDP

The *Centre de Recherche en Droit Public* (CRDP) of the University of Montreal developed an experimental project known as CyberTribunal.[20] It sought to assist parties in both the prevention and resolution of disputes arising in cyberspace. The service tried to address the needs of both businesses and consumers. This experimental projected concluded in December 1999, but the work is continuing via another joint project, the details of which can be found at www.eresolution.ca.

NCAIR

The National Centre for Automated Information Research (NCAIR) has developed the Virtual Magistrate Project and the Online Ombuds Office, to assist parties in the resolution of disputes online.

Virtual Magistrate

The Virtual Magistrate Project[21] offers arbitration between users of online systems that claim to be harmed by posted content and the systems operators. Both parties must consent to the procedure, but the types of complaints are limited to include such issues as copyright infringement, defamation and invasion of privacy.

Online Ombuds Office

The Online Ombuds Office[22] ("OOO") allows users to search their Web site to obtain information that is relevant to their particular dispute. Users can request the assistance of one of the online ombudspersons who do not provide legal advice, but can discuss strategies that a party might employ for the successful resolution of a dispute.

The need for tailored dispute resolution mechanisms for online C to B transfers

Prescribing the dispute resolution process in advance

In order to promote consumer confidence, the service provider, except when acting as consumer, should make clear to which codes of conduct and ADR mechanisms he subscribes, and how information upon these codes and mechanisms can be obtained.

Fostering pragmatism

In B to B contracts, the parties can address their relationship and contract to comply with a dispute resolution process. By contrast, the nature of Web browsing makes it unrealistic to treat dispute resolution as something that the average consumer would intend to address before interacting on the Web. However, in order to foster consumer trust, businesses might well wish to promote and abide by dispute resolution mechanisms.

Considering options

From the earlier discussion of the advantages and disadvantages of dispute resolution mechanisms it seems that litigation, and possibly formal arbitration[23], are "last resort" options, whose effectiveness and adaptability may be limited in respect of online C to B interactions. However, arbitration, modified to look more like the use of a third party arbiter with a simplified set of rules, could have direct application to online C to B dispute resolution.

The other options worth exploring are mediation, med/arb, independent expert evaluation (or expert determination) and conciliation. The latter category is a hybrid of a number of other mechanisms. The exact structure and operation of a conciliation process varies depending on the model and reflects particular types of dispute. The conciliator has the powers of both a mediator and an arbiter. This is distinct from processes such as mediation, which is then escalated to arbitration (med/arb).

Suggestions for developing C to B online alternative dispute resolution mechanisms

Developing dispute resolution for online C to B disputes requires consideration of factors, and the particular characteristics of C to B transfers. Below are some suggestions provided as food for thought.

Use of Privacy Policy Statements

A starting point could be to encourage businesses to inform the consumer of the complaints referral and investigation process they recommend, and to provide guidance on how to invoke these procedures.

Where a business has submitted to a verification process or applied for certification, its adherence to any described dispute resolution mechanism could be one of the matters to be assessed and verified. Verification would have to provide tangible value; it should not be unnecessarily costly or burdensome.

Requirement to exhaust prior remedies

Disputants could be required to exhaust their remedies under the prescribed process, before having recourse to litigation.

There are useful precedents such as industry specific dispute procedures in some jurisdictions, in the areas of insurance, telecommunications, banking and health services. Only after this avenue has been exhausted can the dispute proceed to litigation. Some data protection regimes (such as under the New Zealand privacy law) provide that all complaints must first be referred to the data protection authority for investigation and/or conciliation before they can proceed to the next tier in the dispute resolution process.

Alternatively, encouragement could be given to refer disputes to a dispute resolution service, but not to make this mandatory. Recourse to the court would occur where it is necessary for the data subject or consumer to obtain urgent interlocutory or injunctive relief, such as to prevent a proposed or continuing disclosure of personal data.

Choice of underlying philosophy

A key issue to be discussed is whether alternative C to B dispute resolution mechanisms should be consensual, as in most ADR mechanisms, or provide for a decision-maker with the power to impose a decision. Some options already available are:

- **Independent expert evaluation (determination)**: The parties could nominate an independent third party expert, or else there could be a panel of experts on which to draw.
- **Conciliation**: This is a blend of mediation techniques and adjudicative. The process can draw on an independent expert. The conciliator can issue a recommendation, and sometimes issue an outcome. Alternatively, if the conciliator's recommendation is not followed, the matter is then automatically referred to some other process.
- **A stepped or two-tier process:** The dispute resolution process may commence as mediation but if there is no settlement, the process then converts to arbitration.
- **Online arbitration**.

Other issues to be considered

Many other issues may also need to be considered. Some of those may include:

- The process to log or notify disputes.
- The notification of the parties, including the information to be forwarded to them and the rules governing communications; defining applicable criteria to "hear" the dispute.
- The appointment of any panel of experts.
- The appointment of the Neutral (arbiter/arbitrator/mediator/conciliator/expert).
- The protocols for identifying the information exchanges and any documentary or evidentiary requirements for dealing with the dispute.
- The protocols for establishing a record of the proceedings.
- Confidentiality.
- The security of the communications, and which transmissions must be encrypted.
- Possibilities to co-opt or involve third parties, such as:

  (a) Any data protection authority.
  (b) Any verification agent, inspector or auditor.

- The interface with any self-regulatory action or redress available under a governing industry code or rules.
- The ability or desirability of publishing: binding decisions; anonymised case notes; information providing particular guidance or insights; statistics; reports; the evidence in the proceedings.
- Any power to notify any applicable sector or industry body if the dispute affects a class of individuals or reveals a widespread practice (privacy violation).
- Any limits on the availability of sanctions (such as limits on financial compensation or particular powers of decision-making for the Neutral).
- Where there is no settlement, the advice to the data subject of other avenues of recourse and rights.
- Rules on the enforcement process in respect of any settlement agreement or a final decision or award.
- Self-assessment of the Service. There should be periodic reviews of the statistics for the Service, such as dispute types, resolution outcomes and the reason why some procedures are preferred over others. The results of these reviews should be used to improve the design of the dispute system.

- The volume of disputes which any procedure could handle.
- The simplicity or complexity of the procedure, its timeliness, and cost.
- The possible need for several stages in a procedure between complaints handling and arbitration.

Other questions such as funding, control, oversight, accountability and quality should also be addressed.

Conclusions on dispute resolution mechanisms

Both businesses and consumers need to be able to have confidence in the use of global networks. Both will benefit from an effective mechanism for the resolution of disputes including privacy issues arising in online B-B and B-C transfers. The issues of dispute resolution are critical to improving the level of global privacy protection and development of tailored C to B online dispute resolution mechanisms has to be stimulated.

While some of the traditional mechanisms may be adapted to the resolution of online disputes, it is likely that new mechanisms will need to be developed. Especially in B to C and SME transactions, the cost, speed and enforceability of dispute resolution mechanisms are important considerations.

7. FUTURE INITIATIVES

Summary of conclusions

It arises from the conclusions in this report that there is a role for contractual privacy solutions for transborder data flows occurring in the use of global networks. In particular, the potential of B to B contracts to satisfy the privacy protection expectations as measured against various privacy instruments, must be recognised. However, the report has identified various constraints on the use of B to B contracts. These limitations are not sufficient to negate the validity of privacy contractual solutions as a positive measure, the cumulative effect of which should improve fair information-handling practices and ensure transborder data flows. This is particularly so given the availability of a range of supplementary privacy protection measures.

Many of the B to B contractual issues are relevant to C to B transfers. However, the pressures and characteristics of the GII have significant implications for the use of contractual privacy solutions.

There are a number of initiatives, which have been identified as meriting further consideration. There are four themes, which emerge from the conclusions:

- The importance of promoting privacy awareness and providing educational tools.
- How to develop enforceable privacy commitments for online C to B transfers.
- The various international developments which require monitoring and further collaboration.
- The need to develop online alternative dispute resolution mechanisms for online C to B transfers.

Promoting privacy awareness and educational tools

In accordance with the Openness Principle of the OECD Privacy Guidelines, there should be continued emphasis on systemic measures to improve privacy procedures offering knowledge and/or consent where appropriate to ensure transparency and accountability. Data subjects need to be informed of the purposes of collection and processing of their data. This is a pre-requisite to their ability to challenge the accuracy and use of their data and to being able to pursue their rights, such as seeking redress.

In that respect, the OECD Privacy Policy Statement Generator is a practical measure to provide businesses with the tools to improve their level of awareness of their privacy responsibilities. It also provides the means for businesses (data controllers) to articulate their privacy policy. This educational function should continue to be encouraged; in particular, the correlation between improving consumer confidence and trust in the online environment and ensuring that those responsible for processing personal data act in accordance with the OECD privacy principles.

On the theme of data subject awareness, there may be an opportunity for a dedicated information page resource, made available through the technology (Web site) to inform data subjects of resources regarding laws and/or self-regulatory mechanisms.

Enforceable privacy commitments for online C to B transfers

Much of the data collection occurs prior to the time of formation of any contract. It is very difficult to establish a binding intention to contract, between a consumer browsing a Web site and the data controller of that Web site, until such time as the consumer engages the various prompts to select the goods or services advertised on the Web site, or by providing payment details.

In this context, privacy statements provide an opportunity for data controllers (Web site owners) to put the consumer on notice as to the applicable privacy obligations and as to a number of other matters which support privacy compliance. These may include any verification measures or certification processes applying to the Web site, any submission to the jurisdiction and governing law of a particular country, and the ability to stipulate in advance how complaints will be handled, especially the dispute resolution process.

Attempts to design privacy protection measures within the constraints of a contractual framework may pose difficulties due to the timing issues inherent in, and the nature of, C to B transfers. Even if a privacy statement were held to be a contract, there should be means for the consumer to obtain redress under that contract. There are many difficulties facing any individual consumer or data subject who takes legal action against an online business for breach of privacy through conventional litigation. With the aim of protecting privacy, it may be more efficient to focus less on contractual solutions, and more on dispute resolution measures, in particular on developing creative self-regulatory options in this regard.

Monitoring and collaboration

There are many international developments, which would need to be monitored in order to learn from these experiences when implementing contractual privacy solutions and ancillary measures. The areas to keep under review would include:

- Electronic commerce developments on the contractual requirements for acceptance, non-repudiation and authentication.
- Actual experiences with different forms of verification and certification measures, to assess their practicality, efficacy and benefits.
- Any further work based on the ICC Model Clauses.
- Any work rationalising the rules on conflicts of laws to address the borderless characteristics of the Internet and the difficulty to define territoriality in geographical or physical terms.
- The trend for countries to enact laws to recognise third party beneficiary rights under a contract (to avoid concerns over the lack of privity of contract).
- Any movement towards international co-operation on the legal recognition of statements, declarations or other forms of privacy policies, which would prescribe the dispute resolution processes to be followed.
- The various projects around the world to develop online dispute resolution measures.

Potential framework for encouraging the development of tailored online C to B pilot dispute resolution mechanisms

The importance of individual redress for a privacy breach appears to be a recurring theme. Irrespective of whether or not it is possible to apply a contractual framework to data collection via the Web, the "bottom line" is a pressing need to provide an effective level of privacy protection for consumers in C to B transfers. This includes fostering the opportunity for a consumer or data subject to file a complaint and to have that matter investigated and resolved, without resorting to a very expensive, time-consuming and complex process of issuing court proceedings. There would be corresponding benefits for business in terms of costs and timesavings, possibly greater control over the procedure of dispute resolution, and in increasing credibility and certainty. All of these factors militate in favour of developing self-regulatory alternative dispute resolution mechanisms which could cater for high volume disputes arising out of online C to B transfers.

The development of the Privacy Policy Statement could provide an opportunity to describe how consumer complaints would be handled and any outstanding dispute resolved. A number of mechanisms could be adapted, ranging from mediation (a consensual process) to arbitration (an adjudicative measure).

To conclude, the very nature and scope of the medium in C to B transfers challenges the proposition that a "contract" could solve all the issues. Rather, it should be considered to take a macro approach and develop responses suited to a global privacy protection strategy. The OECD might usefully contribute to future work in this respect by taking forward some of the issues discussed in this report and in particular the study of online dispute resolution mechanisms.

NOTES

[1] The eight Principles are: Collection Limitation Principle; Data Quality Principle; Purpose Specification Principle; Use Limitation Principle; Security Safeguards Principle; Openness Principle; Individual Participation Principle; Accountability Principle.

[2] "Preliminary Views on the Use of Contractual Provisions in the Context of Transfers of Personal Data to Third Countries", 22 April 1998.

[3] http://www.ntia.doc.gov/reports/privacydraft/198dftprin.htm

[4] http://law.gov.au/whatsnew.html

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.

[6] Paras. 37-39; clause 4 Model Contract, http://www.coe.fr-dataprotection/ectype.htm

[7] Comment from page 3, http://www.iccwbo.org/home/statm…ules/rules/1998/model_clauses.asp

[8] FIAT case (1989) and Deutsche Bahn (AG)/Citibank (1995).

[9] Clause 4.

[10] "Preliminary Views on the Use of Contractual Provisions in the Context of Transfers of Personal Data to Third Countries", 22 April 1998.

[11] Brussels Convention 1968 on jurisdiction and the enforcement of judgements in civil and commercial matters. Rome Convention 80/934/CEE 19 June 1980 on the law applicable to contractual obligations 1980.

[12] For example, the ICC Rules of Arbitration provide that the parties "may agree to shorten the various time limits set out in these rules". Rule 32.1, The ICC Rules of Arbitration (in force as of 1 January 1998). Several other arbitral institutions provide for similar procedures with respect to time-frames.

[13] Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York Convention), 10 June 1958, entered into force 7 June 1959.

[14.] In the United States, arbitration decisions can be reviewed by the court to some extent and, as a result, are a matter of public record.

[15] Many organisations, both international and domestic, offer mediation services, and different jurisdictions have laws governing mediation, which can vary widely. To combat the widely disparate body of law on mediation, many entities are seeking to draft model mediation codes or statutes. In the United States, for example, the American Bar Association, in conjunction with the National Conference of Commissioners on Uniform State Laws, drafted a Uniform Mediation Act, which is designed to replace the current mix of state laws on mediation (www.abanet.org/dispute). In Australasia, organisations such as Lawyers Engaged

in Alternative Dispute Resolution (LEADR), and governing bodies of the law profession, have promoted uniformity through codes of ethics.

16 The International Chamber of Commerce offers this service through the ICC International Centre for Expertise. This Centre was created in 1976 and offers the parties the services of a wide variety of experts to assist them in various ways, including assistance in the resolution of disputes.

17 www.truste.org

18 www.bbbonline.org

19 http://arbiter.wipo.int/domains/rules/

20 www.cybertribunal.org .

21 www.vmag.law.vill.edu

22 www.ombuds.org

23 This conclusion assumes that the arbitration model involves the complex and formal procedures of submission to an appropriate arbitration forum.