EUROPEAN COMMISSION
TENDER No. XV/97/18/D

APPLICATION OF A METHODOLOGY DESIGNED TO ASSESS THE ADEQUACY OF THE LEVEL OF PROTECTION OF INDIVIDUALS WITH REGARD TO PROCESSING PERSONAL DATA: TEST OF THE METHOD ON SEVERAL CATEGORIES OF TRANSFER

FINAL REPORT

Presented by The University of Edinburgh on behalf of:

Charles D. Raab
Colin J. Bennett
Robert M. Gellman
Nigel Waters

September 1998

EXECUTIVE SUMMARY

1. This Final Report tests a methodology for assessing the adequacy of the level of protection of individuals with regard to processing personal data. The necessity to assess adequacy is determined by Article 25 of the European Union Data Protection Directive 95/46/EC.

2. Thirty cases of data-transfer are described. The six countries studied are Australia, Canada, China (Hong Kong), Japan, New Zealand and the United States of America. The five categories of transfer reviewed are human resources data, sensitive data in airline reservations, medical/epidemiological data, data in electronic commerce, and sub-contracted data processing.

Summary of Category Conclusions

3. Broad conclusions, generalisable beyond the transfers studied, are difficult to draw in each of the categories. However, on the basis of the cases studied, we concluded:

4. Human Resources Data: Compliance with fair information practices is generally good. At least some elements of fair information principles have been incorporated into practice in all six jurisdictions. In most, many of the necessary elements have been achieved. In each case, this is largely due to the fact that the organisation receiving the transferred data in the destination jurisdiction is a subsidiary of a European parent company.

5. Sensitive Data in Airline Reservations: Compliance with fair information practices is good, as data are collected and used in Europe by European-based airlines under the jurisdiction of European data protection laws. The complexity of the flow of such data, and of the uses to which the data may be put elsewhere, make generalisations difficult about compliance in other jurisdictions, especially where all the fair information principles may not apply. A single transaction may generate multiple data-transfers to multiple players. Passengers with complex flight arrangements that also involve 'special' and other services may find that their data flow through regimes with markedly different levels of privacy protection.

6. Medical/Epidemiological Data: Health care encompasses many associated activities that can occur within organisations besides the health-care provider. Adequate protection for all primary and secondary uses of personal health information is greatly dependent on whether the jurisdiction has a comprehensive data protection law. The adequacy of protection for clinical trial records is heavily dependent on the practices of the company concerned, and particularly on the transfer of personal data in a nearly unidentifiable form.

7. Data in Electronic Commerce: Compliance with fair information practices for the six electronic commerce transfers studied is almost wholly dependent on whether the jurisdiction has a comprehensive data protection law. Where no law applies general fair information practices to electronic commerce activities, electronic commerce is virtually unregulated for data protection. Voluntary industry codes exist in the jurisdictions without applicable laws, but the extent to which those codes address all elements of fair information practices, let alone meet the standards in the EU data protection directive, is highly variable.

8. Sub-Contracted Data Processing: Transfers of personal data between data controllers and data processors pursuant to sub-contracts are for the most part unregulated. It is impossible to offer any general conclusions about the extent to which industry practices meet EU standards, because outside assessors cannot obtain specific information about contracts. However, a full set of protections for data subjects should be available under the law of the EU country in which the data originate. It is unlikely that similar protections are available in third countries, except that security requirements are probably addressed.

Summary of Methodological Conclusions

9. Our experiences in conducting the investigations for this Report are discussed in a methodological conclusion that considers the applicability of the methodology. We also comment upon a range of issues that will be important for any future assessments of this kind, and that should be considered in the implementation of the Directive.

10. Our broadest methodological conclusion is that collecting and analysing information about specific transfers of personal data is not a simple task. In the future, the process of assessing adequacy will require further refinement of analytical instruments for application to a wider array of transfers and circumstances. The institutional machinery for assessing adequacy and for disseminating results will need careful design.

11. We believe that a more empirical analysis of policies and practices, and not just of legal norms and rules, serves both to advance the debate and to anticipate the specific problems that will be encountered in the implementation of the Directive. The assessment of adequacy will be incomplete to the extent that it cannot assess actual practices and the realities of compliance.

12. We outline a number of practical difficulties in applying the methodology for assessing adequacy. These concern the extent and consistency of organisations' co-operation with investigations, variations in the reliability of information elicited by the inventory of questions, the variety of areas of business to be found in a single organisation, legal uncertainties and jurisdictional differences. Assessment problems also arise over determining the applicability of data protection rules to anonymised data, and over the inseparability of data derived from the EU and from the third-country held in the same database.

13. A further complication arises from the lack of clear priority amongst the criteria to be applied in the assessment of adequacy. This may provide useful flexibility in the decision-making process, but it also leaves judgements open to argument. Differences in culture and in institutional functioning may cloud the issue of determining the extent of adequacy.

14. The methodological conclusion considers a number of transitional questions that may be important in the coming years, and which may affect the assessment of adequacy. We also enumerate longer-term considerations concerning the effect of risk assessment, commercial confidentiality and the nature of complaints processes on the way determinations of adequacy are initiated and carried out. We suggest that the assessment process itself has a beneficial effect on organisational learning by data controllers and others, and needs to be regularised. Attention should be given to the institutional arrangements within and beyond the European Union for the assessment of adequacy and the establishment of an 'intelligence capability' for this task.

TABLE OF CONTENTS

I. INTRODUCTION

1. We were contracted to test a methodology for assessing the adequacy of the level of protection of individuals with regard to processing personal data in six non-European Union (EU) countries, and with respect to five categories of data-transfer.

2. The six countries are Australia, Canada, China (Hong Kong), Japan, New Zealand and the United States of America.

3. The five categories of transfer are sub-contracted data processing, human resources data, medical/epidemiological data, data in electronic commerce, and sensitive data in airline reservations.

4. Member States are required to implement the EU Data Protection Directive 95/46/EC in national law. This includes legislating provisions relating to transborder data flow to 'third countries' (Article 25(1):

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

5. The basis for the assessment of adequacy is found in Article 25(2):

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

6. By design, this study did not consider the derogations available under Article 26(1) of the Directive. Little would be learnt from case studies if the derogations for consent or for the interests of the subject ((a) and (b)) were applied too broadly, since the questions of adequacy would not arise. It remains to be seen how the concept of 'free and informed consent' will be applied in interpretation of these derogations. This Report does, however, touch on the derogation provided by Article 26(2), since the Article 29 Working Party has made it clear that contracts designed to satisfy Article 26(2) should meet the same criteria of adequacy as for assessments under Article 25[1]. This is particularly relevant in the sub-contracting cases where contractual terms appear to be the main means of providing privacy protection in relation to most of the jurisdictions studied.

7. Our First Report (February 1998) described, for each category, our progress and thinking concerning the specific transfers that we then intended to investigate in detail. We proposed to use the methodology outlined by the European Commission in its 'First Orientations' paper[2] and elaborated by the analytical framework described in our response to the tender.

---

[1]European Commission, DG XV/D/5005/98/final, Working Party on the Protection of Individuals With Regard to the Processing of Personal Data, WP9, Working Document: Preliminary Views on the Use of Contractual Provisions in the Context of Transfers of Personal Data to Third Countries', adopted by the Working Party on 22 April 1998.

[2]European Commission, DG XV D/5020/97-EN final, Working Party on the Protection of Individuals With Regard to the Processing of Personal Data, WP4, 'First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy', adopted by the Working Party on 26 June 1997. At a late stage in our work, a subsequent document, DG XV D/5025/98 WP12, 'Transfers of Personal

8. Our Second Interim Report (June 1998) and its Supplement (July 1998) together gave provisional descriptions of the application of the methodology to 18 transfers.

9. This Final Report describes the application of the elaborated methodology to all 30 transfers. It also arrives at substantive and methodological conclusions concerning the assessment of adequacy in non-EU countries. The Appendix reproduces the analytical framework - an inventory of questions - that was used in gathering information for the transfers.

10. In Section II of this Report, we describe the cases within each of the transfer categories. The cases are based on actual or typical transfers, placed within hypothetical descriptive scenarios that conform to reality. In most categories, the cases share the same scenario in terms of the nature of the transfer of data from the European Union, and therefore are reported in a fairly uniform way, with variations where relevant. Because different readers will read this Report in different ways - by category or by country, or simply with interest in one or a few cases, - we thought it advisable to repeat the scenario in each case rather than stating it only once in a generic scenario for a particular category of transfer. For reasons of confidentiality, we have invented fictitious names of organisations in order to conceal their identities as far as possible; any resemblance of names to actual organisations is unintentional.

11. Although each case ends with brief conclusions, we also summarise the conclusions for each category of data transfer. This fulfils a secondary aspect of our remit, which was to draw some substantive conclusions about the adequacy of data protection from our findings. The brevity of these category conclusions reflects the lack of a firm basis for a more extensive final assessment, given the limited nature of the evidence gathered. In addition, pronouncements on the adequacy of particular countries in regard to particular types of transfer were not the main rationale for the present study.

12. Section III contains a longer assessment of the methodology used in this Report, and explains our experiences in using it, with a view to how others might approach the task of assessing adequacy. This was regarded from the outset as the main objective of the study. We believe that the lessons learnt in the course of carrying out this study will be of considerable interest in carrying out more effective and incisive investigations and determinations of adequacy.

13. The Appendix contains the inventory of questions used as a guide for data collection.

14. We should like to acknowledge the constructive advice we have received from officials of DG XV in refining our approach to the subject. They have also clarified a number of issues that arose both from the terms in which the relevant Articles of the Data Protection Directive 95/46/EC are written, and from the alternatives left open by the 'First Orientations' paper and other documentation. We have also benefited from their comments and suggestions following the previous Reports.

15. We have received useful assistance from informants and other contacts in most of the non-EU countries concerned, as well as in EU countries. Because we gave undertakings to persons in organisations involved in data transfers that we would not identify them or their organisations, we can only acknowledge our indebtedness to them in an aggregate and anonymised way. We have also been assisted by privacy commissioners and other senior officials in supervisory authorities, and by other knowledgeable individuals, in many countries and jurisdictions. These include Australia, Canada, Hong

---

Data to Third Countries: Applying Articles 25 and 26 of the EU Data protection Directive', was adopted by the Working Party on 24 July 1998. It synthesised WP4 and other Working Party documents of relevance to the question of transfers to non-EU countries.

Kong, Japan, New Zealand, The Netherlands, the United Kingdom, the United States, the Australian Capital Territory, British Columbia, Manitoba and Quebec. Neither they nor our informants bear any responsibility for the contents of this Report. We would also like to acknowledge the help of Cory Basbaum with the translation of Japanese materials.

16. Finally, it may also be appropriate here, if a bit unusual, to acknowledge the value of the means of electronic communication, without which a study of this kind would have been impossible in such a relatively short time. The location of the four members of the research team in the United Kingdom, Canada, the United States and Australia facilitated the gathering of information about transfers to different jurisdictions, but made the process of analysing, collating and reporting the results almost entirely dependent on electronic mail and fax communication. Except for very brief meetings of different combinations of the four members, all the work was carried out in 'cyberspace'. To the extent that we have gained a greater appreciation of the possibilities of electronic communication, so we have also realised with greater clarity the potential dangers to privacy inherent in its use. We hope that this Report helps to ensure that the potential of these media is realised in a way which safeguards privacy.

II. THE CASES

1. In this section, we describe and analyse cases of the transfer of personal data to the six non-European Union countries: Australia, Canada, China (Hong Kong), Japan, New Zealand, and the United States of America. The cases are presented within the five categories of types of transfer. These are human resources data, sensitive data in airline reservations, medical/epidemiological data, data in electronic commerce, and sub-contracted data processing.

2. Each case is described under main headings, some of which have sub-headings. The main headings normally used are:

The Nature and Circumstances of the Transfer
Overview of the Regulatory Environment for This Case
Purpose Limitation, Transparency and Opposition
Data Quality and Proportionality
Security
Access and Rectification
Onward Transfer Restrictions
Remedies
Accountability
Conclusions

3. The Appendix contains questions that were used selectively as a general guide for collecting information in each case.

4. A brief conclusion about each category follows the cases in that category.

5. A common scenario concerning the transfer of data to the third country is described for most or all of the cases in each category, before the privacy protections provided in that country are analysed. There are variations of the categorical scenario among the human resources and medical/epidemiological cases.

Human Resources Data

(a) *Australia*

The Nature and Circumstances of the Transfer

1. ANTIPODEAN BANK is an Australian bank which is part of a group which includes a European bank. Executives based in the European Union are occasionally transferred to Australia for periods of employment that may last several years. For purposes of this case study, it is assumed that an employee of the European bank has been seconded to work at ANTIPODEAN in Brisbane, Queensland, Australia for two years. He will be bringing his partner and school-age children to live in Australia.

2. ANTIPODEAN's Human Resources office receives information on transferred employees from the employees' 'home' organisation, and directly from the employee concerned.

3. The Bank also handles the necessary applications for visas and permits, which involve some personal information being provided directly by the employee, by completing forms, and some from the bank as the employer. The employee obtains a temporary resident visa.

4. Most of the Bank's employees are also its customers, and they receive staff discounts or special terms on accounts and financial products.

Overview of the Regulatory Environment for This Case

5. There is currently no general privacy law in any Australian jurisdiction. The federal (Commonwealth) Privacy Act 1988 applies to the activities of a bank relating to the provision of consumer credit, but only applies to the Human Resources or personnel record-keeping practices of organisations in the very narrow area of use of the government issued Tax File Number (TFN). There are also statutory controls on the use of records of 'spent' criminal convictions.

6. Government policy since 1997 has been not to legislate for privacy protection in the private sector generally, but to encourage industry self-regulation. The Privacy Commissioner has been conducting a consultative process to develop National Principles for the Fair Handling of Personal Information (NPs) which could be used as the basis either for legislation (which now seems likely in the state of Victoria), or for self-regulatory codes. The Commissioner issued a set of Principles in February 1998, covering all of the core areas of privacy, providing rules about collection, use and disclosure, quality, security and access and correction, and designed to be in line with international best practice, although some aspects are currently under review. Several business groups have committed themselves to incorporate the Commissioner's Principles in voluntary codes of practice, with associated compliance and complaint handling mechanisms. The Victorian government has also said that it will adopt the Commissioner's Principles as the basis of its statutory regime, to be introduced into Parliament later in 1998.

7. The state of Queensland, of which Brisbane is the capital city, used to have a statutory Privacy Committee with a general Ombudsman function, but with no binding principles or compliance or enforcement mechanisms. The Privacy Committee Act of 1984 lapsed in 1991. Since then several official reports have recommended more comprehensive privacy legislation. Most recently, a Queensland Parliamentary Committee report in May, 1998 recommended that egislative protection for privacy should apply to the state public sector, but that privacy in the private sector should be left to the current federal government

initiative to develop a consistent national scheme. The federal government's position is that this scheme can be achieved on a voluntary self-regulatory basis.

8. ANTIPODEAN is a member of the Australian Bankers Association (ABA) and subscribes to the national Banking Code of Practice, and to the banking industry's self-regulatory dispute resolution scheme involving the Banking Industry Ombudsman. ANTIPODEAN is also subject to a code of conduct for Electronic Funds Transfer. The ABA has announced plans for all members to adopt the Privacy Commissioner's National Principles (NPs) in relation to their customers, and to set up a mechanism for compliance monitoring, enforcement and dispute resolution, on a self regulatory basis. It is however still unresolved whether the NPs, either generally or in the banking context, will apply to employee data.

9. A committee of the national standards organisation, Standards Australia (SA), is developing a standard for 'Personal and Corporate Data - Representation and Management'. This standard has reportedly been drafted with privacy principles and Human Resources data in mind, but it has yet to be issued for public comment. No compliance or enforcement machinery attaches to SA Standards. Unless they are incorporated into legislation, the standards are merely guidance that can be adopted on a voluntary basis.

10. The ANTIPODEAN group also has a world-wide internal 'code of conduct' and ANTIPODEAN BANK in Australia has a Human Resources Instruction manual that includes some data protection standards with general guidance on the collection, use, maintenance, and disclosure of personal data on employees.

11. The International Labour Organisation (ILO) issued a code of practice in 1996 entitled 'Protection of Workers' Personal Data', giving guidance on how to apply internationally recognised privacy principles in the employment and workplace context. Although official Australian representatives were closely involved in the development of the Code, it has only advisory status and the government has not made any formal commitment to implementing the Code in Australia.

Purpose Limitation, Transparency and Opposition

Collection

12. The information received about the employee arrives either by fax, e-mail or post, and is entered into the local Human Resources database, and a paper file is also created. A detailed medical report is also required; the employee arranges an examination in his home country and has the report sent as hard copy to ANTIPODEAN's Human Resources department where it is filed separately.

13. The information held about employees is determined to a large extent by the design of ANTIPODEAN Bank's local Human Resources computer system. The system has standardised fields for name, address, company identification number; date of birth and marital status (for visa and health insurance purposes); job history, and salary history and performance information only for the period of employment by ANTIPODEAN. There is also a field for the government TFN but in accordance with the statutory TFN Guidelines issued under the federal Privacy Act, this is kept separate from the general personnel file and accessible only by staff working on payroll or taxation aspects.

14. Employees could be assumed to have some general awareness that data are being transferred in connection with their transfer. However, the details of the transfers and the identity of all organisations receiving data may not be fully transparent, although individuals would be told if they asked.

15. All ANTIPODEAN employees in Australia have from time to time been told something about their personnel files - for instance when the TFN requirements have changed, but there has been no comprehensive notification along the lines that would be required by most privacy laws. The transferred European employee is not given any specific information about the Human Resources record keeping practices on his arrival.

Use and disclosure for ANTIPODEAN Bank purposes

16. ANTIPODEAN uses Human Resources information for the usual range of personnel related purposes, including for payroll, resource planning, performance appraisal, and to provide employees with information. There are also leave and training records, which are held separately from the general records and performance appraisal reports. Some of these uses necessarily involve incidental disclosures to third parties, e.g., to other banks for making salary payments.

17. ANTIPODEAN, like other group companies, offers a range of employee benefits that include health insurance and life insurance and a pension. In this case, ANTIPODEAN would take over responsibility for making payments into the employee's existing pension and life insurance funds in Europe, but this would be administered through his 'home' bank, and not require any direct contact between ANTIPODEAN and the funds. ANTIPODEAN would enrol the employee and his family in a local Australian health insurance scheme.

18. In addition to the regular personnel information maintained on all employees, the Human Resources department assists transferred executives in finding housing and schools. Records necessary to support these services are maintained separately. There will obviously be a range of necessary incidental disclosures involved in the provision of these services, e.g., to schools, real estate agents, licensing and registration authorities. Provided these disclosures are only of the amount and type of information necessary, these will be made with either the express or implied consent of the employee.s

19. The bank does not regard other members of the banking group as third parties, and will exchange customer information with other business areas such as insurance, investment products, and travel agencies. These exchanges are currently limited but ANTIPODEAN is increasingly exploring the potential of sharing information within the group and is considering a major data warehousing project which would centralise customer records and facilitate matching and profiling for marketing purposes. Since all employees have access to staff discounts, they are considered at least potential customers and included in prospect databases. Employees are not given any choice about this, although there is an occasional notice about the scheme in staff newsletters.

Disclosure to third parties for other purposes

20. ANTIPODEAN will need to pass on some of the employee 's personal information to the local health insurance fund. This will be done presumably with his informed consent.

21. ANTIPODEAN's policy is not to disclose customer information to third parties outside the banking group for commercial purposes. They will not sell or rent customer lists, which include some information about employees, most of whom have accounts with the bank and take advantage of discounted loans. The bank is a member of the Australian Direct Marketing Association (ADMA) which already has some clauses relating to personal information in its 'standards of practice' and has announced plans to adopt the NPs and to set up a semi-independent code-administration committee to deal with disputes.

22. Other Australian laws (federal and state) require employers to routinely provide information about salaries and tax deductions to the tax authorities, and certain information to the Immigration Department. Various government officials have a statutory right to

information upon demand, e.g.: for enforcement of labour and health and safety laws; while law enforcement bodies can obtain warrants in the course of investigations. Banks are subject to additional reporting requirements in relation to investment income and financial transactions, but these are relevant to customer information rather than employee records.

23. The policy of ANTIPODEAN BANK is only to disclose personnel information when required by law, or with the express consent of the individual. Information requested by the police would as a matter of policy only be disclosed in response to a formal warrant, and only after consultation with the bank's legal department. The possibility of disclosure in response to less formal requests for assistance is currently being discussed in the context of the Privacy Commissioner's NPs.

24. Most federal government agencies receiving personal data from the bank will be subject to the general Information Privacy Principles of the Privacy Act 1988, but state and local government agencies are not subject to any general privacy requirements.

25. The Australian Banking Code of Practice has a clause about confidentiality of customer records which reflects the well-established common-law bankers' duty of confidence in relation to financial affairs. While the ABA has argued strongly that this provides sufficient privacy protection, many observers doubt if it adequately covers disclosures which a bank itself feels are in the customers' interests, such as for marketing services from related companies. In any case, the Code and the common-law duty do not apply to employees' personal information, and do not therefore assist in relation to the transfer in this case.

Data Quality and Proportionality

26. There are no statutory obligations concerning data quality, other than those relating to consumer credit under the Privacy Act.

27. ANTIPODEAN BANK relies heavily on employees themselves to ensure the quality of factual personal information. Every year, employees are a print-out of their own Human Resources database record to check and update.

28. The quality of personal information is further maintained, indirectly, by sharing it with employees, for instance during annual performance-appraisal reviews.

Security

29. ANTIPODEAN BANK's information security department is part of its computer operations division. Understandably, the main focus of attention is on the security of customer information and of financial transactions. Human Resources records benefit incidentally from the general emphasis given to security. For Human Resources records, company policies determine which employees may access which records. A personal profile determines which computer screens an employee may view and which the employee may update.

30. Human Resources files are not encrypted. Audit trails record changes to records, but not 'read only' access that does not involve a change (provided the viewer has the appropriate authority). If an employee requests access to a file that the employee is not entitled to see, the attempt is recorded as a security violation and may result in an investigation.

31. ANTIPODEAN BANK has internal guidelines on how long to keep data, whether to microfilm data for archives, and on disposal methods.

Access and Rectification

32. No statutory rights of access or correction apply to private-sector businesses in Queensland. Within ANTIPODEAN BANK, requests for correction of personnel files and appeals or disputes about Human Resources records are rare. ANTIPODEAN's employee privacy policy does recognise the right of employees to view most of their personnel record, and to file notices of disagreement, for instance with supervisor's appraisals. The company has no policy about notifying third-party recipients when a record has been corrected.

Onward Transfer Restrictions

33. There are no statutory restrictions on the transfer of personal information to other jurisdictions, whether inside Australia or overseas. If the banks carry out their intention to adopt the Privacy Commissioner's National Principles as a voluntary code to be given effect in customers' contracts, then this will include an onward transfer principle (NP9) aimed at ensuring that privacy protection is not lost when data is transferred overseas. However, if the principles are implemented on a sub-national basis, as in the banking sector, this principle will need to be re-drafted to apply to any transfers within Australia.

Remedies

34. Currently, the only areas of personal-information handling by Australian banks that are subject to statutorily enforceable remedies are the use of consumer-credit information and of TFNs. In both of these areas, individuals (including temporary residents) can complain to the Federal Privacy Commissioner about breaches of the statutory rules and can be awarded remedies, including compensation in appropriate cases. Remedies following complaint investigations can however only be enforced by order of the Federal Court, which would necessitate a de-novo hearing of the case if a respondent refused to be bound by the Commissioner's determination. The TFN jurisdiction applies to bank employees both as employees and as customers, while the credit jurisdiction only applies to those of them that are also customers.

35. Breaches of the Banking Code of Practice can be taken up with the Banking Industry Ombudsman, who can make determinations which are binding on the bank concerned, including awarding settlements and/or compensation of up to $150,000 to individual consumers. The Code currently only incorporates the principle of confidentiality, and applies only to customers and not to employees. If the banks adopt the NPs, the Banking Ombudsman's jurisdiction is likely to be extended to the whole range of privacy issues in relation to customers, but it is unlikely to extend to employee privacy complaints (other than in their capacity as customers).

36. Some disclosures by a bank could also be a breach of their common-law duty of confidence, and individuals could pursue common law remedies through the civil courts, although the cost of doing so would almost certainly be prohibitive unless there was an associated major financial loss. Again, these are remedies available only to individuals in their capacity as bank customers, not as employees.

37. In relation to the disclosure of personal information involved in setting up a health insurance policy for the employee and his family, health insurance funds in Australia are subject to a statutory complaints scheme, the Private Health Insurance Complaints Commissioner, but her jurisdiction does not currently expressly extend to privacy issues. Only in the Australian Capital Territory are there statutory rules about the handling of personal health information, under the 1997 Health Records (Privacy and Access) Act.

Accountability

38. The ANTIPODEAN BANK privacy policy is available on request to all bank employees. No specific privacy training is conducted, but relevant responsibilities would be covered as part of routine training.

39. Employees are not currently required to sign a non-disclosure agreement, but misuse of personal information - of staff as well as customers - would be grounds for disciplinary action.

40. Bank activities are subject to regular internal and external audits. In the Human Resources area the internal audit program covers compliance with the general Human Resources Instructions and Code of Conduct, and specifically addresses access to confidential data. Any violations of security detected during routine monitoring would be the subject of further investigation.

41. There is a general company grievance process which would be used for any complaints about breaches of employee privacy.

Conclusions

42. Some elements of fair information practices have already been incorporated, voluntarily, in the human resource policies of ANTIPODEAN BANK.

43. Neither federal nor Queensland laws expressly give employees (whether of a bank or any other private sector organisation) any privacy rights in connection with their employment relationship (other than in relation to the government TFN, and spent convictions). Employees do not have access to any complaint mechanisms for privacy matters (other than in relation to TFNs, 'spent' convictions, or, if they are also customers, credit information), beyond the bank's internal grievance procedure.

44. The bank has committed itself to some privacy principles through adoption of various codes of practice, such as the Banking Code, the Electronic Funds Transfer Code and the Direct Marketing Standards of Practice. It is likely to extend these commitments in the near future to the full range of privacy principles if the ABA's and ADMA's plans to adopt the Privacy Commissioner's National Principles are implemented. Some of these commitments are also carried through into dispute resolution machinery, including the Banking Industry Ombudsman scheme. However, most of these commitments relate only to customer personal information and do not apply to personnel records.

Human Resources Data

(b) *Canada*

The Nature and Circumstances of the Transfer

1. CANSUB is a Canadian subsidiary of an international bank with headquarters in the United Kingdom. Executives based in the European Union are routinely but occasionally transferred to Canada for periods of employment that may last several years. CANSUB's Human Resources office located in Toronto, Ontario receives information on transferred employees from the CANSUB head office as well as from the employee concerned. The information is integrated into the Human Resources database controlled by the Toronto office. The company does not maintain personnel data on a computer network accessible to offices in other countries. For purposes of this case study, it is assumed that an employee of the European bank has been seconded to work at CANSUB in Toronto for two years. She will be bringing her partner and school-age children to live in Toronto.

2. In addition to the regular personnel information maintained on all employees, the Human Resources office has a special area for transferred executives that assists them in finding housing and schools. Records necessary to support these services are maintained separately.

3. The Bank also handles the necessary applications for visas and permits, which involve some personal information being provided directly by the employee, by completing forms, and some from the bank as the employer. The employee obtains a temporary employment visa from Canada Immigration.

Overview of the Regulatory Framework for This Case

4. No federal or provincial legislation establishes general data protection standards regulating the processing of personnel information anywhere in Canada, except in Quebec. Ontario, like all other provinces, has a public-sector Freedom of Information and Protection of Privacy Act (FOIPPA) dating from 1987, overseen by the Ontario Information and Privacy Commissioner, which only regulates provincial government agencies. Information on salaries and benefits paid will be transmitted to Revenue Canada for the withholding of taxes, and will then be subject to the federal Privacy Act of 1982, overseen by the federal Privacy Commissioner.

5. In Canada, financial institutions are regulated at either the federal or provincial level. All banks are federally incorporated and are therefore federally regulated. All securities dealers, credit unions and *caisses populaires* are provincially incorporated and registered, and are therefore provincially regulated. Trust, loan and insurance companies may be either federally or provincially regulated, depending on the jurisdiction under which the company chooses to incorporate. A Canadian subsidiary of a foreign bank, therefore, is a federally regulated institution overseen by the Office of the Superintendent of Financial Institutions (OSFI).

6. The relevant legislation overseen by OSFI is the Bank Act. 1997 Amendments to this legislation empower the Governor-in-Council to make regulations 'requiring a company or society to establish procedures regarding the collection, retention, use and disclosure of any information about its customers or members or any class of customers or members.' No such regulations have yet been issued. In any case, it is unclear whether an employee's information would be covered by these provisions, or whether such an employee could complain to OSFI for any breach of privacy.

7. For legal standards that might govern the collection and processing of employee information by CANSUB, one must look more to provincial laws enacted for other purposes and with a more general application beyond the financial sector. For example, the Employment Standards Act requires an employer to keep records of the employee's name and address, hours of work, wages and gross earnings, deductions made, net amount paid to the employee and documents relating to leave. An employer must also maintain records of an employee's name, address, wage rate, vacation, hours worked and actual earnings under the Industrial Standards Act. The Employment Equity Act requires employers to establish and maintain records concerning designated group membership (gender, minority ethnic groups, etc.) and employment history. If our executive were also a shareholder in CANSUB, then the Corporations Act would require the company to keep a list of shareholders and shares owned and to make it available to other shareholders, members and creditors of the corporation.

8. No codes of practice govern this type of information. For consumer-related information, CANSUB would certainly be expected to abide by the principles within the Canadian Bankers Association's (CBA) 1996 'Privacy Model Code', a sectoral code of practice based upon the Canadian Standards Association's 'Model Code for the Protection of Personal Information'. The CBA is currently developing a parallel code of practice for employees, but to date nothing has been published. The recently tabled federal Bill C-54 will apply to the personal information about an employee that the organisation processes in connection with the operation of a federal work, undertaking or business.

9. At the moment, however, the data protection policies of CANSUB are internally developed and implemented, and consistent with company procedures world-wide. Executives transferred to Canada become part of the Human Resources database just like Canadian employees. The same general policies that apply to the records of Canadian employees apply to records of transferred executives. The company has an internal 'employee privacy policy' as part of its Human Resources policy manual that establishes data protection standards with general guidance on the collection, use, maintenance, and disclosure of personal data on employees. CANSUB maintains personnel records for payroll, benefit and incentive purposes, and those requirements (together with external legal requirements) direct the collection, maintenance, and use of employee information.

Purpose Limitation, Transparency and Opposition

Collection

10. The information received about the employee arrives either by fax, e-mail or post, and is entered into the local Human Resources database, and a paper file is also created. A detailed medical report is also required; the employee arranges an examination in her home country and has the report sent as hard copy to CANSUB's Human Resources department, where it is filed separately.

11. Employees could be assumed to have some general awareness that data are being transferred in connection with their move to Canada. However, the details of the data transfers and the identity of all organisations receiving data may not be fully transparent, although individuals would be told if they asked. The transferred European employee is not given any specific information about the Human Resources record-keeping practices on her arrival. There would be no comprehensive notification along the lines that would be required by most privacy laws.

Use and Disclosure for CANSUB purposes

12. CANSUB uses Human Resources information for the usual range of personnel-related purposes, including payroll, benefits management, resource planning, performance

appraisal, and the provision of information for employees. As required by federal and provincial laws, the company withholds taxes from salary paid to employees and transmits both taxes and information to federal and provincial tax authorities. All individuals receiving wages must complete state and federal forms that direct the tax withholding process. The forms are distributed and used by employers to determine how much tax should be withheld. Each employee is also provided with a Social Insurance Number, used as the identifier for all revenue-related purposes in Canada. The information held about employees is determined to a large extent by the design of CANSUB's local HR computer system. The system has standardised fields for name, address, company identification number; date of birth and marital status (for visa and health insurance purposes); job history, and salary history and performance information only for the period of employment by CANSUB.

13. CANSUB offers traditional employees' benefits that include health insurance, pensions, and life insurance. A variety of health plans are available to employees, and the processing of claims for health products and services is accomplished by the plans and not by the company. Other benefits selected by employees may require the sharing of information with outside organisations that provide or manage the benefits. Because employees select benefits, they have some awareness that data are being transferred in order to provide the benefit. However, the details of the transfers and the identity of all organisations receiving data may not be fully transparent. In this case, CANSUB would take over responsibility for making payments into the employee's existing pension and life insurance funds in Europe, but this would be administered through her 'home' bank, and not require any direct contact between CANSUB and the funds.

Disclosure to third parties for other purposes

14. CANSUB will need to pass on some of the employee's personal information to the local health insurance fund. This will be done presumably with her informed consent. Information may be disclosed in response to requests for employment verification or for credit-related verification (e.g., application for a mortgage). In these instances, employee consent is a prerequisite for the disclosure. The Ontario Consumer Reporting Act would also regulate the collection and disclosure of credit reports, and the operations of credit reporting agencies; the credit-reporting industry is regulated by similar statutes in most provinces.

15. In addition to the regular personnel information maintained on all employees, the Human Resources department assists transferred executives in finding housing and schools. Records necessary to support these services are maintained separately. There will obviously be a range of necessary incidental disclosures involved in the provision of these services, such as to schools, real estate agents, licensing and registration authorities. Provided these disclosures are only of the amount and type of information necessary, these will be made with either the express or implied consent of the employee.

16. CANSUB's policy is not to disclose customer information to third parties outside the bank group for commercial purposes – i.e., they will not sell or rent customer lists, which will include some information about employees, most of whom have accounts with the bank and take advantage of discounted loans. The bank is a member of the Canadian Bankers' Association whose code of practice contains clauses relating to the use of personal information for marketing purposes.

17. Other Canadian laws (federal and provincial) require employers to routinely provide information about salaries and tax deductions to the tax authorities and certain information to the Canada Immigration. Various government officials have a statutory right to information upon demand, e.g.: for enforcement of labour and health and safety laws; while law enforcement bodies can obtain warrants in the course of investigations. Information requested by the police would, as a matter of policy, only be disclosed in response to a formal warrant, and only after consultation with the bank's legal department. Federal government agencies receiving personal data from the bank will be subject to the

Privacy Act of 1982. Any Ontario agency will be subject to Ontario's Information and Privacy legislation.

Data Quality and Proportionality

18. Requirements for data accuracy, relevance, timeliness, and completeness are internal to the company. Some information, such as home address and telephone numbers, can be accessed and corrected directly by employees. Employees can also view other information from their own personnel files, including salary, benefits, and other data. Access to these records is regulated by password controls supplemented by a requirement for entry of the employee's Social Insurance Number.

19. The quality of other information is further maintained by sharing it with employees on a regular basis. In connection with an annual review for merit pay increases, a computer-generated document is printed and sent to each employee, who is asked to confirm name, address, identification numbers, job history, and similar data from the personnel records. This annual review affords the data subject an opportunity to confirm or correct the data in the personnel record.

20. In addition, prior to the enrolment period for company benefits, each employee receives a form that shows demographic and dependent information. The purpose is to make sure that appropriate benefits are available to each employee. The process provides another opportunity for review and correction of employee data.

21. Finally, managers conduct annual personnel reviews with each employee, and the employee signs the resulting review. This affords an opportunity for each employee to discuss and appeal the review with his or her manager. The Human Resources office receives and maintains the results of that process.

Security

22. CANSUB has an information-security department that is part of its computer operations division. In addition, each division within the company has its own security officer. For Human Resources records, company policies determine which employees may access which records. A personal profile determines which computer screens an employee may view and which the employee may update.

23. Human Resources files are not encrypted. Audits trails track some file activities. The computer system will record who updated a file although it does not record access without change. However, when an employee requests access to a file that the employee is not entitled to see, the attempt is recorded as a security violation and may result in an investigation.

Access and Rectification

24. No statutory rights of access or correction apply to private-sector businesses in Ontario. CANSUB's employee privacy policy does recognise the right of employees to view most of their personnel record, and to file notices of disagreement; for instance, disagreements with supervisors' appraisals. The company has no policy about notifying third-party recipients when a record has been corrected.

Onward Transfer Restrictions

25. Except for demands from federal and provincial governments, personnel files are not routinely transferred to third parties. When an employee who was transferred from Europe returns to another job in Europe or in a bank office in another country, the employee's personnel information returns to London. The London office then forwards the information to the new location.

Remedies

26. Remedies for aggrieved employees are very hard to find in Ontario. Unlike British Columbia and some other provinces, Ontario does not have any legislation setting out a general tort for privacy invasion. Unlike Quebec, there is no general data protection statute, covering the private sector. The federal Charter of Rights and Freedoms does not contain an explicit right to privacy, even though Section 8 reads: 'Everyone has the right to be secure against unreasonable search and seizure.' But the Charter applies only to the Government of Canada and to the legislature and government of each province.

27. Remedies that are specific to the banking industry have very little relevance for bank employees. The privacy regulations under the Bank Act, the CBA's Model Privacy Code and the system of complaints mediation through the banking ombudsman apply almost entirely to business or individual customers. Bill C-54 provides for a complaints-resolution mechanism through the Office of the Federal Privacy Commissioner.

28. For the most part, therefore, employees have no simple and direct way to enforce fair information practices. For the most part, personal information is used inside organisations in ways that are not visible to the outside world or to the subject of the information. Whether a CANSUB employee could sue to force the company to comply with its stated privacy policy is uncertain.

Accountability

29. A written employee privacy policy for Human Resources records addresses many of the elements of fair information practices in general terms. The policy is available to all bank employees. The policy reflects a general policy of limited internal use and limited external disclosure. Employees have a right to access and to correct their records. Security is a required element, and misuse of personal information can result in the dismissal of an employee. Standards for accuracy are also included. Records that are being disposed must be shredded. Each employee of the Human Resources must sign a non-disclosure agreement.

30. The Senior Vice-President for Human Resources oversees privacy policy for Human Resources records. That person may be the equivalent of a privacy officer. Staff training in the bank's privacy policy is conducted routinely as part of other training activities for Human Resources employees.

31. Bank activities are subject to annual external audits and internal reviews. The bank conducts no reviews specifically focused on compliance with privacy requirements, but violations of security recorded during routine monitoring may be the subject of further investigation during other reviews, including any investigations by the OSFI.

Conclusions

32. Many of the elements of fair information practices are incorporated in the policies of CANSUB. Employees receive notice of privacy policies, have the ability to see and correct

many, if not most, of their personnel records. The bank has policies addressing limiting both use and external disclosure. The personnel computer system limits the collection and maintenance of some information simply by not having the capacity to store the data. Security protections are in place.

33. These practices are guided neither by statutory privacy protections, nor by general industry guidelines on banking information or on Human Resources data. In this respect, the situation in Ontario is generally similar to that in every other province and territory with the exception of Quebec.

34. If CANSUB were located in Quebec, aggrieved individuals would probably be able to lodge a complaint with the *Commission d'Accès à l'Information* (CAI), the supervisory authority that oversees both public-sector and private-sector privacy-protection legislation. The CAI would probably try to mediate a settlement under these circumstances, and would make no distinction between Quebec and non-Quebec complainants. There is still, however, a constitutional question about the extent to which their regulatory power extends to federally regulated institutions and whether or not the CAI would be able to investigate or audit banking institutions that constitutionally fall under the federal jurisdiction.

35. When Bill C-54 comes into force, employee records such as those maintained by CANSUB will be regulated, and subject to the investigative and oversight powers of the Federal Privacy Commissioner. Employee records, however, that are not under the control of federally regulated industries will escape the reach of C-54, and of the Privacy Commissioner.

Human Resources Data

(c) *Hong Kong*

The Nature and Circumstances of the Transfer

1. FIRST ORIENT is a Hong Kong bank which is part of a group which includes a European bank. Executives based in the European Union are occasionally transferred to the Hong Kong for periods of employment that may last several years. For purposes of this case study, it is assumed that an employee of the European bank has been seconded to work at FIRST ORIENT Bank in Hong Kong for two years. She will be bringing her partner and school-age children to live in Hong Kong.

2. FIRST ORIENT's Human Resources (Human Resources) office receives information on transferred employees from the employee's 'home' organisation, and directly from the employee concerned. The bank also handles the necessary applications for visas and permits, which involve some personal information being provided directly by the employee, by completing forms, and some from the bank as the employer.

3. Most of the Bank's employees are also its customers, for they receive staff discounts or special terms on accounts and financial products.

Overview of the Regulatory Environment for This Case

4. The FIRST ORIENT Bank is subject to the Hong Kong Personal Data (Privacy) Ordinance, and must comply with the six data protection principles. The Ordinance is a comprehensive data protection law covering both the private and public sector, and establishing the Office of the Privacy Commissioner for Personal Data to administer and enforce the law. The Commissioner has issued supplementary guidance about the application of the Ordinance to Human Resource Management (Fact Sheet 2, May 1997), and is preparing a Code of Practice, but this will not be complete until sometime in 1999.

5. FIRST ORIENT is a member of the Hong Kong Institute of Human Resource Management (IHRM), which has issued 'Guidelines on Personal Data Privacy' to assist members to comply with the Ordinance. The FIRST ORIENT Group has a world-wide internal 'code of conduct' and FIRST ORIENT Bank in Hong Kong has an Human Resources instruction manual that include some data protection standards with general guidance on the collection, use, maintenance, and disclosure of personal data on employees.

6. FIRST ORIENT Bank is a member of the Hong Kong Association of Banks, and has adopted the non-statutory 'Code of Banking Practice'. However, this Code applies only to dealings with personal customers and the privacy provisions in the Code do not therefore apply to employee data.

Purpose Limitation, Transparency and Opposition

Collection

7. The information received, usually by fax or mail, is entered into the local Human Resources database and a paper file is also created. A worldwide group Human Resources database is under development but not yet implemented. A detailed medical report is also required; the employee arranges an examination in her home country and has the report sent as hard

copy to FIRST ORIENT's Human Resources department where it is filed separately.

8. The information held about employees is determined to a large extent by the design of FIRST ORIENT Bank's local Human Resources computer system. The system has standardised fields for name, address, Hong Kong Identity Card Number, company identification number, date of birth and marital status (for work permit and health insurance purposes), job history (for transferred employees, this would only be about the immediately preceding job), and salary history and performance information only for the period of employment by FIRST ORIENT. This accords with the IHRM Guidelines which also warn against the collection of particularly sensitive information such as religion and political affiliations.

9. Employees could be assumed to have some general awareness that data are being transferred in connection with their secondment. However, the details of the transfers and the identity of all organisations receiving data may not be fully transparent, although individuals would be told if they asked.

10. All FIRST ORIENT employees in Hong Kong have been informed about the records that are held about them and about the rules of the Privacy Ordinance. The European employee would not specifically be given this information on arrival, although the Privacy Commissioner's office would expect that she should.

Use and disclosure for FIRST ORIENT Bank purposes

11. FIRST ORIENT uses Human Resources information for the usual range of personnel-related purposes, including payroll, resource planning, performance appraisal, and the provision of information for employees. There are also leave and training records, which are held separately from the general records and performance appraisal reports. Some of these uses will necessarily involve incidental disclosures to third parties, e.g., to other banks for making salary payments.

12. All routine uses and disclosures by a Human Resources department in carrying out its functions are likely to be seen as either part of the original purpose for which the information was collected, or a directly related purpose, and therefore in accordance with Data Protection Principle (DPP) 3 of the Ordinance. The Human Resources Fact Sheet explains that most routine access to personnel files - for instance by supervisors, appraisers and internal auditors - would be consistent with this principle and would therefore not need the employee's consent.

13. FIRST ORIENT, like other group companies, offers a range of employee benefits that include health insurance, life insurance and a pension. In the employee's case, FIRST ORIENT would take over responsibility for making payments into her existing European pension and life insurance funds, but this would be through her 'home' organisation and not require any direct contact between FIRST ORIENT and the funds. FIRST ORIENT would enrol the employee and her family in a local (Hong Kong) health insurance scheme. The health insurance fund concerned happens to be a subsidiary of the bank, but there is a 'firewall' between the two systems, and FIRST ORIENT's Human Resources department would only be able to obtain details of medical matters with the employee's consent, and will need to supply the fund only with the gender and date of birth of the employee and members of her family. Again, all of these uses and disclosures would be consistent with DPP3.

14. In addition to the regular personnel information maintained on all employees, the Human Resources department assists seconded executives in finding housing and schools. Records necessary to support these services are maintained separately. There will obviously be a range of necessary incidental disclosures involved in the provision of these

services, e.g., to schools, real estate agents, licensing and registration authorities. Provided these disclosures are only of the amount and type of information necessary, these will be made with either the express or implied consent of the employee.

15. If FIRST ORIENT decides to send marketing offers to employees, the IHRM Guidelines remind the company that it should clearly explain this and offer employee the opportunity to opt out, in accordance with s.34 of the Ordinance.

Disclosure to third parties for other purposes

16. Other Hong Kong laws require employers to provide information routinely about salaries and tax deductions to the tax authority - the Inland Revenue - and certain information to the Immigration Department. Various government officials have a statutory right to information upon demand, e.g., for enforcement of labour laws or health and safety, while law enforcement bodies can obtain warrants in the course of investigations.

17. The policy of FIRST ORIENT Bank is only to disclose personnel information when actually required to by law, or with the express consent of the individual. Information requested by the police may be disclosed without a formal warrant (taking advantage of the 'reasonable grounds - likely to prejudice' exception in the Privacy Ordinance (s.58)), but only after consultation with the legal department**.**

18. Nearly all potential recipients of personal data in Hong Kong will themselves be data users subject to the Privacy Ordinance, so the data will continue to have the same protection as it enjoys within the bank, having regard to the 'authorised' uses which recipients may be able to make of it. For many government agencies this will be set out in other laws.

Data Quality and Proportionality

19. The quality of other information is further maintained by sharing it with employees on a regular basis; for instance base data are confirmed with employees during the annual performance appraisal review.

20. The information held by FIRST ORIENT about employees may include trade-union memberships, which is defined in the EU Directive as ‘special’ (i.e., sensitive). There are no specific requirements in the Hong Kong Ordinance providing additional protection for sensitive data. However, in practice, it would seem that details of trade-union membership are held with the express consent of the employee or, if not, for the purpose of complying with employment law. Both of these are exemptions acknowledged by the Directive for sensitive data (Article 8(2)(a) and (b)).

21. DPP2 of the Hong Kong Ordinance forbids data users to keep personal data for any longer than is necessary for the fulfilment of any legitimate purpose. This should lead organisations to review their data management practices and institute record disposal programmes. FIRST ORIENT Bank has internal guidelines on how long to keep which types of data, whether to microfilm it for archives, and on disposal methods. FIRST ORIENT Bank is seeking clarification that they are able to keep records in certain circumstances such as, for example, where an employees has been dismissed for dishonesty.

Security

22. The Hong Kong Ordinance requires data users to take all practicable steps to protect personal data against unauthorised or accidental access, processing, erasure or other use

(DPP4). The IHRM Guidelines contain some practical suggestions about the steps that should be taken.

23. FIRST ORIENT Bank's information security department is part of its computer operations division. In addition, each division within the company has its own security officer. For Human Resources records, company policies determine which employees may access which records. A personal profile determines which computer screens an employee may view and which the employee may update.

24. Human Resources files are not encrypted. Audit trails record changes to records, but not 'read only' access that does not involve a change, if the viewer has the appropriate authority. However, when an employee requests access to a record that the employee is not entitled to see, the attempt is recorded as a security violation and may result in an investigation. There are internal bank guidelines on record disposal.

Access and Rectification

25. The Hong Kong Privacy Ordinance creates a right of access for individuals to information about themselves, subject to a range of exemptions, and provides correction rights and a process for challenging refusal of access (DPP6). The exemptions include some which are specific to employee data, including personal data relating to staff planning intentions and some personal references. The Hong Kong Privacy Ordinance requires FIRST ORIENT Bank to ensure that personal data are accurate (DPP2). FIRST ORIENT Bank relies heavily on employees themselves to ensure the quality of factual personal information. Existing policies in relation to personnel information go a long way towards meeting the access and correction obligations of DPP6. Employees do not have direct access on-line to any of their own personnel records, but at least every two years they are sent a print-out of the records to check and update.

26. Requests for correction of personnel files and appeals of disputes are rare. The employee privacy policy does recognise the right of employees to file notices of disagreement when necessary. The company has no policy about notifying third-party recipients when a record has been corrected.

Onward Transfer Restrictions

27. Section 33 of the Hong Kong Ordinance will prevent data users from transferring personal data outside Hong Kong unless certain conditions are met, with the aim of ensuring that the data will be continue to be protected and handled in accordance with privacy principles. This Section is not yet in force. The Privacy Commissioner has issued further guidance on this provision (Fact Sheet 1, May 1997).

28. When s.33 is brought into force, data users such as FIRST ORIENT Bank will be able to transfer data freely to any places which have been specified by the Privacy Commissioner as having similar laws, without any further steps. It seems likely that European Union (EU) member states will be declared to have similar laws, and therefore transfers about a European employee back to her home country will not pose any difficulty. But if the FIRST ORIENT Bank wants to transfer information about her to a 'third country' which has not been specified, it will only be able to do so if:

- it has reasonable grounds for believing that there is a similar law in force (in the absence of any guidance from the Privacy Commissioner);
- it has obtained the employee's consent in writing;
- it is in her interests but in circumstances where consent is impracticable to obtain (but likely);
- the use or disclosure involved is an exempt one for the purposes of DPP3; or

- the data user has taken reasonable precautions and exercised ‘all due diligence’ to ensure the data will be handled responsibly.

Fact Sheet 1 suggests that one way of demonstrating 'due diligence' is to use contract terms, and a model contract is included. The FIRST ORIENT Group's Code of Conduct, which applies world-wide to all personal data handled within the Group, could serve the same purpose as a contract.

29. The inclusion in the Hong Kong law of an 'onward transfer' provision, similar in terms and effect to Articles 25 and 26 of the EU Directive, would appear to satisfy one of the core requirements which EU members are likely to require in order to assess a place as having adequate protection, once s.33 is in force. The breadth of the DPP3 exemptions as applied to s.33 would seem at first sight to weaken the effectiveness of s.33 as a safeguard, but are in fact analogous to the exception provided by Article 26(1)(d) of the Directive.

Remedies

30. FIRST ORIENT Bank has a general company grievance process which would be used for any complaints about breaches of employee privacy. Under the Hong Kong Privacy Ordinance, employees can complain to the Privacy Commissioner about alleged breaches of any of the privacy principles. This right applies to any individual about whom data are held; they do not have to be Hong Kong citizens or even residents. A temporarily resident foreign national would clearly enjoy all the rights given to individuals under the Ordinance.

31. The Commissioner's staff can assist the complainant and try to mediate. If this is unsuccessful, an investigation can lead to the Commissioner’s issuing an enforcement notice, directing the data user to take specified action, and/or instigating prosecution. Contravention of an enforcement notice is an offence which can result in a fine or imprisonment. The Ordinance creates a right of action for compensation for damage or distress, although individuals would have to bring such action in the civil courts.

Accountability

32. The FIRST ORIENT Bank’s privacy policy is available on request to all bank employees. This accords with the recommendations of the IHRM Guidelines. No specific privacy training is conducted, but relevant responsibilities would be covered as part of routine training; the IHRM Guidelines suggest that there should be specific privacy training and communications. Employees are not currently required to sign a non-disclosure agreement.

33. Bank activities are subject to regular internal audits, although in the Human Resources area only the pension scheme is subject to external audit. The internal audit programme covers compliance with the general Human Resources Instructions and Code of Conduct, and specifically addresses access to confidential data. Any violations of security detected during routine monitoring would be the subject of further investigation.

34. Some privacy breaches may also be breaches or offences under other laws and other remedies and penalties may apply.

35. The Privacy Commissioner also has a pro-active monitoring role under the Ordinance and proposes to commence a programme of inspections (audits) later in 1998.

Conclusions

36. Many of the elements of fair information practices have already been incorporated in the human resource policies of FIRST ORIENT Bank. It is now required in Hong Kong to comply with the Data Protection Principles of the Personal Data (Privacy) Ordinance, and employees, including foreign nationals, have legal rights under the Ordinance. The Ordinance has also created a comprehensive system of supervision, compliance monitoring and enforcement through the Office of the Privacy Commissioner for Personal Data.

37. The collection, use and disclosure policies of the FIRST ORIENT Bank in Hong Kong would seem at first sight to be consistent with their obligations of the Personal Data (Privacy) Ordinance.

38. Once the onward transfer provisions of s.33 are in force, the privacy protection regime in Hong Kong as it applies to the handling of Human Resources data by a business operating in Hong Kong would appear to meet all the main requirements that have been suggested as necessary to be assessed as 'adequate' for the purposes of Article 25.

Human Resources Data

(d) *Japan*

The Nature and Circumstances of the Transfer

1. The INTERNATIONAL BANKING GROUP (IBG) is a multinational conglomerate of different financial institutions. The Human Resource department in its headquarters in Eurostate, a member state of the European Union, has developed a large and comprehensive database on about 500 current employees at the managerial level.

2. EASTFUND is the Japanese subsidiary of IBG, which wants to find a senior executive to handle a particular set of operations for the next five years. They ask IBG's human resources manager for the dossiers of possible candidates. The Human Resources department in Eurostate searches its database according to the search criteria specified by EASTFUND. The search yields ten qualified persons. The Human Resources manager then prints their dossiers and sends them to Tokyo by international courier. EASTFUND then makes a decision about a short list of three candidates for personal interview.

3. This case raises the question of the protection of the personnel records whilst they are located in Japan. It is assumed that once an appointment has been made, the dossiers of the 9 unsuccessful candidates are then returned to Eurostate. This analysis focuses entirely on the protections afforded to the information that is transferred during the search process, and excludes information that might be generated (for taxation, insurance, housing and education needs) once an appointment has been made and an executive has decided to relocate.

Overview of the Regulatory Environment for This Case

4. There is presently no law governing the protection of employee's personal data in Japan, even though the Ministry of Labour has been discussing the passage of employee personal information protection guidelines since 1997. At the moment, therefore, EASTFUND is subject to no general data protection law covering the private sector. Nor does any sectoral legislation apply specifically to Japanese financial institutions. No provisions relating to the protection of personal information can be found embedded in recent banking legislation (http://www.cebu-online.com/japanlawbase/bfirst.htm). Personal data protection is not apparently an issue that has so far been included in Japanese law on labour standards (http://www.tuj.ac.jp/law/lawresources.html#translations).

5. The Center for Financial Industry Information Systems (FISC) has issued 'Guidelines on the Protection of Personal Data for Financial Institutions' in March, 1987 (revised March, 1991). FISC was incorporated in 1984 as a non-profit organisation under the aegis of the Ministry of Finance. Originally based on the OECD Guidelines of 1980, the FISC Guidelines are currently being reviewed and revised. The FISC Guidelines are intended to apply to all financial institutions, including banks, insurance companies, credit card companies and securities companies. Although the guidelines make no distinction between personal data about customers and about employees, representatives of FISC confirm that they were only intended to cover customer-related information. To the extent that they oblige general policies on information security and accountability, however, they will probably have some unintended consequences for the processing of employee records.

6. The data protection practices of EASTFUND are, therefore, totally dependent on the policies that have been internally developed and implemented within the IBG group. IBG has a Code of Conduct that applies worldwide. All personal data handled within the

Group, including data transferred to Group companies in other countries, is handled according to the centrally determined Human Resources policies.

Purpose Limitation, Transparency and Opposition

Collection

7. The Human Resources database of IBG holds data on the top 500 managers who work worldwide and who are career-mobile. The database has a common format and composite record for each person, including name, address, date-of-birth, gender, marital status, educational qualifications, dependants and their names and relation to the person, languages spoken and a digitised photograph. There are data on the employee's experience (coded by functions and countries worked in), as well as the coded performance appraisal record. Other notes (from previous interviews) might also be included. The database does not hold information on health history, handicaps, religion, ethnicity, trade-union membership or criminal record.

8. Employees could be assumed to have some general awareness that data are being transferred in connection with this personnel search. Employees have a copy of their dossiers and sign off once a year that they have checked them.

Use and disclosure for EASTFUND purposes

9. Use of these dossiers is strictly controlled by company policy. They should only be used for the purposes of selecting an individual for this particular position. They should be circulated to company personnel only on a 'need to know' basis. The dossiers of unsuccessful candidates should be returned to Eurostate at the completion of the search.

Disclosure to third parties for other purposes

10. Disclosure of personnel files outside the company is strictly controlled by IBG policy, even though no law or code practice governs personal information disclosures in Japan.

Data Quality and Proportionality

11. The IBG Group companies rely heavily on employees themselves to ensure the quality of factual personal information. Employees do not have direct access online to any of their own personnel records, but at least every year they are sent a print-out of the records to check and update. The quality of other information is further maintained by sharing it with employees during the annual performance-appraisal review. These data should be kept no longer than is necessary to complete the search.

Security

12. EASTFUND has an information security department that is part of its computer operations division. In addition, each division within the company has its own security officer. For Human Resources records, company policies determine which employees may access which records. When an employee requests access to a file that the employee is not entitled to see, the attempt is recorded as a security violation and may result in an investigation. There are internal bank guidelines on record-disposal.

13. This may be one area where the FISC Guidelines have some applicability. They require financial institutions to use 'reasonable security safeguards against such risks as

unauthorised access, loss, destruction, modification, leakage etc.' Security system requirements are also included in a separate set of 'Computer System Security Guidelines for Financial Institutions', produced by FISC in December, 1985 (revised February, 1991). These Guidelines, although rather old, contain detailed guidance on physical security, hardware/software security and procedural security.

Access and Rectification

14. No provision in Japanese law entitles employees to have access to their own employment records. If executives wished to access and correct their files, this would presumably be done in Eurostate, and before the transfer to Japan. The employee privacy policy of IBG does recognise the right of employees to file notices of disagreement when necessary. The company has no policy about notifying third-party recipients when a record has been corrected.

Onward Transfer Restrictions

15. No provision in Japanese law pertains to the onward transfer of personal information. There appears to be no other external limitation on EASTFUND's ability to transfer employee records to other jurisdictions.

Remedies

16. There might be plausible circumstances under which an employee whose application was rejected would wish to file a complaint or grievance with EASTFUND, which does have a general company grievance process that would be used for any complaints about breaches of employee privacy.

17. Remedies external to the company are, however, very difficult to find. The consumer complaints process recently established through the Ministry of Trade and Industry (MITI) (and discussed in the Japanese Electronic Commerce case elsewhere in this Report) is intended to apply solely to consumer data. It is very unclear whether an employee complaint could be resolved through this regime. It is also clear that the award of 'Privacy Marks' is intended to reassure consumers rather than employees about the propriety of that company's personal information handling practices.

18. The courts would also be almost inaccessible. It is worth noting in this context Japan does not have a sufficiently large number of legal professionals to support even a fraction of the litigation common to European countries, not to mention the United States. Going to court to claim a right is therefore never an option that the Japanese would be likely to consider. The number of civil suits per capita brought before the courts is roughly one-twentieth of the figures for common-law countries. Virtually all cases of civil conflict are settled by conciliation, either out of court or before a judicial verdict is reached. Given the different cultural role for the law in Japan, the ability of a foreign national to seek and find redress under this system is extremely remote, if not unheard of.

Accountability

19. The 1991 revision of the FISC Guidelines includes a brief section on 'Accountability'. Each financial institution is expected to appoint a 'person who is competent to decide about the handling of personal data' for complying with the contents of the guidelines. In November, 1990, the FISC published a Manual for the Further Management of Personal Data for Financial Institutions as a checklist on the proper handling of personal data.

20. EASTFUND's activities are subject to regular internal audits. The internal audit programme covers compliance with the general Human Resources Instructions and Code of Conduct, and specifically addresses access to confidential data. Any violations of security detected during routine monitoring would be the subject of further investigation.

Conclusions

21. As a subsidiary of a foreign-owned bank, EASTFUND’s practices are directed by worldwide company policy rather than by local Japanese laws and codes. For the brief time that files a transferred from IBG in Eurostate for the purposes of completing a specific search, there appears to be a good level of compliance with data protection principles.

22. External controls are, however, absent. The FISC Guidelines are out-of-date and incomplete in some respects. They contain no provision for external complaints resolution and were not devised with bank employees in mind. There appears to be no other applicable code or sectoral law that would apply to the personal data transferred to a company like EASTFUND from overseas. New initiatives from MITI are focused more on providing reassurances to consumers (especially in an online environment) than to protecting the privacy rights of employees. The Japanese system is not, therefore, able to deliver help and support to data subjects nor to offer remedies, if those within the company fail.

Human Resources Data

(e) *New Zealand*

The Nature and Circumstances of the Transfer

1. SOUTHSEAS is a New Zealand bank which is part of a group which includes a European bank. Executives based in the European Union (EU) are occasionally transferred to New Zealand for periods of employment that may last several years. For purposes of this case study, it is assumed that an employee of the European bank has been seconded to work at SOUTHSEAS Bank in New Zealand for two years. He will be bringing his partner and school-age children to live in New Zealand.

2. SOUTHSEAS' Human Resources office receives information on transferred employees from the employees' 'home' organisation, and directly from the employee concerned. The Bank also handles the necessary applications for visas and permits. These involve some personal information being provided directly by the employee by completing forms, and some from the bank as the employer. The employee is granted a temporary resident visa.

3. Most of the Bank's employees are also its customers, for they receive staff discounts or special terms on accounts and financial products.

Overview of the Regulatory Environment for This Case

4. SOUTHSEAS Bank is subject to the New Zealand Privacy Act 1993, which includes both privacy standards (11 Information Privacy Principles, or IPPs) and enforcement and complaint mechanisms. After a transitional period, the Act has been fully in force since 1996. The New Zealand Privacy Commissioner has issued a considerable amount of guidance material for businesses on compliance with the Act, and a wide range of training has been offered. The New Zealand Privacy Act makes provision for sector or activity codes of practice which can substitute for the 'default' principles, but there have been no such codes issued to date that affect SOUTHSEAS' activities. The bank subscribes to the New Zealand Banking Association's Code of Banking Practice, but this applies only to dealings with customers, not employees.

5. The International Labour Organisation (ILO) issued a code of practice in 1996 entitled 'Protection of Workers' Personal Data' giving guidance on how to apply internationally recognised privacy principles in the employment and workplace context, but this has not been taken up in any official context in New Zealand. The New Zealand Institute of Personnel Management has issued guidance notes on compliance with the Privacy Act. SOUTHSEAS Bank itself has an Human Resources instruction manual that includes some data protection standards with general guidance on the collection, use, maintenance, and disclosure of personal data on employees, reflecting the requirements of the Privacy Act.

Purpose Limitation, Transparency and Opposition

Collection

6. The information about the employee and his family is received from Europe, either by fax, e-mail or post, and is entered into the local Human Resources database. A paper file is also created. A detailed medical report is also required; the employee arranges an examination in his home country and has the report sent as hard copy to SOUTHSEAS' Human Resources department where it is filed separately.

7. The information held about employees is determined to a large extent by the design of SOUTHSEAS Bank's local Human Resources computer system. The system has standardised fields for name, address, company identification number; date of birth and marital status; job history; and salary history and performance information since the employee has been with the group.

8. Employees could be assumed to have some general awareness that data are being transferred in connection with their movement overseas. However, the details of the transfer may not be fully transparent, although the employee would be told if he asked.

9. All SOUTHSEAS employees in New Zealand have been informed generally about the records that are held about them and about their rights under the Privacy Act, in compliance with IPP 3. The employee will be given this information on arrival in New Zealand.

Use and disclosure for SOUTHSEAS Bank purposes

10. SOUTHSEAS Bank uses Human Resources information for the usual range of personnel-related purposes, including payroll, resource planning, performance appraisal, and to provide employees with information. There are also leave and training records, which are held separately from the general records and performance-appraisal reports. Some of these uses will necessarily involve incidental disclosures to third parties, e.g., to other banks for making salary payments.

11. All routine uses and disclosures by an Human Resources department in carrying out its functions are likely to be seen as either part of the original purpose for which the information was collected, or as a directly related purpose, and therefore in accordance with IPPs 10 and 11 of the Privacy Act. Most routine access to personnel files - for instance by supervisors, appraisers and internal auditors - would be consistent with this principle and would therefore not need the employee's consent. The medical report on the employee is held separately and would not be available for most of these purposes.

12. SOUTHSEAS, like other group companies, offers a range of employee benefits that include health insurance, life insurance and a pension. In this case, SOUTHSEAS would take over responsibility for making payments into the employee's existing pension and life insurance funds in Europe, but this would be through his 'home' employer in the EU and would not require any direct contact between SOUTHSEAS and the funds. SOUTHSEAS would enrol the employee and his family in a local (New Zealand) health-insurance scheme.

13. In addition to the regular personnel information maintained on all employees, the Human Resources department assists transferred executives in finding housing and schools. Records necessary to support these services are maintained separately. There will obviously be a range of necessary incidental

disclosures involved in the provision of these services, e.g., to schools, real-estate agents, licensing and registration authorities. Provided these disclosures are only of the amount and type of information necessary, these will be made with either the express or implied consent of the employee.

14. The bank does not regard other members of the parent group as third parties, and will exchange information with other business areas such as insurance, investment products, and travel agencies. These exchanges are currently limited but SOUTHSEAS Bank is increasingly exploring the potential of sharing information within the group and is considering a major data warehousing project which would centralise customer records and facilitate matching and profiling for marketing purposes. To the extent that most employees are also customers, this issue is relevant to the transfer of the employee.

Disclosure to third parties for other purposes

15. SOUTHSEAS Bank will also need to pass on some of the employee's personal information to the local health insurance fund. This will be done presumably with his informed consent.

16. SOUTHSEAS Bank's policy is not to disclose customer information to third parties outside the bank group for commercial purposes - i.e., they will not sell or rent customer lists. The bank is a member of the New Zealand Direct Marketing Association which already has some clauses relating to personal information in its 'standards of practice'.

17. Other New Zealand laws require employers routinely to provide information about salaries and tax deductions to the Inland Revenue (the tax authority), and certain information to the Immigration Department. Various government officials have a statutory right to information upon demand, e.g., for enforcement of labour laws or health and safety, while law enforcement bodies can obtain warrants in the course of investigations.

18. The general policy of SOUTHSEAS Bank is to disclose personnel information only when required by law, or with the express consent of the individual. Information requested by the police may be disclosed without a formal warrant (taking advantage of the 'maintenance of the law' exception to IPP 11), but the Bank's policy is to do this only after consultation with its legal department.

19. As nearly all potential recipients of personal data in New Zealand will themselves be agencies subject to the Privacy Act, so the data will continue to have the same protection as they enjoy within the Bank, having regard to the 'authorised' uses which recipients may be able to make of the data; for many government agencies these will be set out in other laws.

20. Most other organisations to which SOUTHSEAS Bank may transfer personal information about the employee within New Zealand are subject to the same requirements of the Privacy Act as the bank itself. The Health Insurance Fund is subject to the Health Information Privacy Code 1994 - a code issued under the Privacy Act which varies the privacy principles - called Rules in the Code - for the circumstances of health care. The complaints, compliance and enforcement mechanisms of the Privacy Act continue to apply.

Data Quality and Proportionality

21. The New Zealand Privacy Act requires SOUTHSEAS Bank to take reasonable steps before using personal information to ensure that it is accurate, up-to-date, complete, relevant and not misleading (IPP 8). SOUTHSEAS Bank relies heavily on employees themselves to ensure the quality of factual personal information. Employees do not have direct access on-line to any of their own personnel records, but at least every two years they are sent a print-out of the records to check and update.

22. The quality of other information is further maintained by affirmatively sharing it with employees on a regular basis. For instance, routine data are confirmed with employees during the annual performance appraisal review.

23. IPP 9 of the New Zealand Act limits data users from keeping personal data for any longer than is necessary for the fulfilment of any legitimate purpose. This should lead organisations to review their data management practices and institute record disposal programs. SOUTHSEAS Bank has internal guidelines on how long to keep which types of data, whether to microfilm it for archives, and on disposal methods.

Security

24. The New Zealand Privacy Act requires data users to apply reasonable safeguards to protect personal data against loss, unauthorised or accidental access, use modification or disclosure, and other misuse (IPP 5).

25. SOUTHSEAS Bank's information security department is part of its computer operations division. In addition, each division within the company has its own security officer. For Human Resources records, company policies determine which employees may access which records. A personal profile determines which computer screens an employee may view and which the employee may update.

26. Human Resources files are not encrypted. Audit trails record changes to records, but not 'read only' access that does not involve a change, if the viewer has the appropriate authority. However, when an employee requests access to a file that the employee is not entitled to see, the attempt is recorded as a security violation and may result in an investigation.

Access and Rectification

27. Access and correction rights are granted by the Privacy Act 1993 forpersonal information held by all private sector organisations, including banks. These rights apply equally to customer and employee records (IPPs 6 and 7), although unlike the other principles, they do not apply to non-residents unless they are in the country. Therefore, the European employee would enjoy these enforceable rights only while he was actually in New Zealand.

28. Like most large New Zealand businesses, SOUTHSEAS Bank has established processes for the receipt and processing of access requests. There have been several hundred requests since the access right commenced, but these have mostly been from customers. Only a handful of employees have made formal Privacy Act requests for access, and requests for correction of personnel files and appeals of disputes are even rarer. The employee privacy policy does recognise the right of employees (under IPP 7(3) of the Act) to file notices of disagreement.

29. The Act also requires organisations to inform third parties to whom they have disclosed personal information, if reasonably practical, of any corrections or additions that are made subsequently in response to a challenge from an individual. Whether SOUTHSEAS' Human Resources department would keep adequate records and remember to do this is a hypothetical compliance issue.

30. While SOUTHSEAS Bank would be likely to give any existing or former employee the same access and correction rights as a matter of company policy, even if they were overseas, a non-resident would not be able to pursue any dispute through the Privacy Commissioner.

Onward Transfer Restrictions

31. The New Zealand Privacy Act does not currently contain any provisions which restrict the transfer of personal data outside New Zealand. The Commissioner, in his recent review of the Act, invited submissions as to whether such a provision was needed (partly in light of Article 25 of the EU Directive). The Commissioner is expected to issue his report on the Review in October, 1998. In relation to the present case, however, it is difficult to see many situations in which data about the employee would be transferred to a third country without his consent, and it is not therefore a significant factor.

Remedies

32. SOUTHSEAS Bank has a general company grievance process which would be used for any complaints about breaches of employee privacy, and although this would not prevent an employee from exercising his or her rights under the Privacy Act directly, the Commissioner encourages complainants to try to obtain a remedy from internal processes first, if at all possible.

33. Under the New Zealand Privacy Act, employees can complain to the Privacy Commissioner about alleged breaches of any of the privacy principles. This right applies without qualification to New Zealand citizens and permanent residents, but access and correction rights (IPPs 6 and 7) only apply to non-residents while they are actually in New Zealand.

34. The Commissioner's staff can assist an employee to try to conciliate or mediate the complaint. If this is unsuccessful, the Commissioner can refer the matter to a separate Proceedings Commissioner, who will in turn decide whether to take the case to the Complaints Review Tribunal. The Tribunal can make an order prohibiting a repetition of the action complained about, and/or require the interference with privacy to be put right. The Tribunal can also require the respondent agency to pay damages or compensation.

35. It should be noted that very few complaints proceed as far as the Tribunal; most are resolved at an earlier stage. Also, there is a substantial complaints-handling backlog due to resource constraints, with individuals typically having to wait twelve months for investigation of their matter to even begin, unless it is assessed as urgent.

36. In relation to employment matters, some privacy complaints typically involve other grievances, and an individual may choose to have a complaint handled under the Employment Contracts Act, which gives recourse to an Employment Tribunal.

Accountability

37. The SOUTHSEAS Bank privacy policy is available on request to all bank employees. No specific privacy training is conducted, but relevant responsibilities would be covered as part of routine training. SOUTHSEAS would be likely to draw the policy to the attention of the employee in the present case, who is transferring from overseas, as he could not be assumed to be familiar with New Zealand law.

38. Employees are not currently required to sign a non-disclosure agreement. Under New Zealand employment law, deliberate misuse of personal information, about staff as well as customers, would generally be held to be reasonable grounds for disciplinary action or, if serious enough, dismissal

39. SOUTHSEAS Bank activities are subject to regular internal and external audit. The internal audit programme covers compliance with the general Human Resources Instructions, and specifically addresses access to confidential data. Any violations of security detected during routine monitoring would be the subject of further investigation.

40. Apart from his complaints investigation role, the Privacy Commissioner also has a range of pro-active promotional and compliance monitoring functions under the Privacy Act but has neither the formal powers nor the resources to conduct a systematic privacy-audit programme. He can undertake audits at the request of organisations, but not uninvited.

Conclusions

41. SOUTHSEAS Bank in New Zealand has been required for five years to comply with the Information Privacy Principles of the Privacy Act, and the elements of fair information practices have been incorporated in the human resource policies of SOUTHSEAS Bank. Employees, including foreign nationals, have a range of entitlements under the Act. The Act has also created a comprehensive system of supervision, enforcement through the Privacy Commissioner (lacking only a pro-active audit role), and an associated complaints-review machinery (although the complaints backlog is disturbing).

42. Personal information about an EU employee seconded to work at SOUTHSEAS Bank is therefore protected by law in a way which in most respects meets the test of adequacy envisaged by the Article 29 Working Party in relation to Article 25 of the EU Directive, at least while he or she was in New Zealand. The absence of a comprehensive onward transfer provision in the law would only be an issue in this case study if personal information about the employee were sent on to a third country without his consent, and this seems unlikely. As the law stands, employees would also lose access and correction rights once they left New Zealand, although a large organisation such as a bank could be expected to continue to provide access in accordance with company policy.

Human Resources Data

(f) *United States of America*

The Nature and Circumstances of the Transfer

1 AMFUND is an American subsidiary of an international bank with headquarters in the European Union. Executives based in Europe are routinely but occasionally transferred to the United States for periods of employment that may last several years. AMFUND's Human Resources office located in the State of New York receives information on transferred employees. The information is integrated into the Human Resources database controlled by the New York office. The company does not maintain personnel data on a computer network accessible to offices in other countries. For purposes of this cased study, it is assumed that the employee has been sent to work at a company office located in New York. He will be bringing his partner and school-age children to live in New York.

2. AMFUND maintains Human Resources files for payroll purposes, to manage benefits, to provide employee information, and for other standard employment and administrative purposes. As required by state and federal laws, the company withholds taxes from wages paid to employees and transmits taxes and related information to state and federal tax authorities. All individuals receiving wages must complete state and federal forms that direct the tax withholding process. Employers distribute the forms to employees and use the information collected to determine the amount of tax withholding.

3. AMFUND offers traditional employees benefits that include health insurance, pensions, and life insurance. A variety of health plans are available to employees, and the processing of claims for health products and services is accomplished by the independent health plans and not by the company. The company does not maintain any health data as part of human resources records. This is not the case with all American employers. Many process health claims on behalf of their insurers or have self-funded insurance plans. The availability of health data within companies is a common and sometimes controversial practice. Other benefits selected by AMFUND employees may require the sharing of information with outside organisations that provide or manage the benefits. Because employees select benefits, they have some awareness that data are being transferred in order to provide the benefit. However, the details of the transfers and the identity of all organisations receiving data are not fully transparent. Local AMFUND employees receive no specific disclosures about information sharing with benefit providers. Transferred employees receive no local benefits so information sharing is not an issue.

4. In addition to the regular personnel information maintained on all employees, the Human Resources office has a special area for transferred executives that assists them in finding housing and schools. Records necessary to support these services are maintained separately.

Overview of the Regulatory Environment for This Case

5. No federal workplace law establishes general data protection standards regulating the processing of personnel information. Federal laws enacted for other purposes create some rights and responsibilities for employee or applicant information. State laws also sometimes establish standards for the processing of employee information. The result is a patchwork quilt of laws covering aspects of personnel information processing. For example, both federal and New York State labour laws require employers to maintain records of employees, wages, and similar information. The laws also require employers to provide the information upon demand of government officials responsible for labour laws. In theory, federal or state departments of labour could exercise oversight of employer data

protection practices, but comprehensive oversight is unlikely. Oversight of specific workplace statutes will touch on data protection issues on occasion.

Purpose Limitation, Transparency and Opposition

6. Some laws limit the ability of employers to collect or use information about job applicants. Examples of these laws include the federal Americans with Disabilities Act, the federal Fair Credit Reporting Act, and the New York State law prohibiting unlawful workplace discrimination. The legal restrictions are generally not relevant to the transfer of personnel already employed by the bank and transferred to the United States.

7. Other laws place demands on employers to collect and disclose information about employees. Federal, state, and sometime local tax laws require American companies to withhold income and social security taxes from wages and to report information regularly to tax and social security authorities. Pension laws and anti-discrimination laws also require companies to conduct their operations in accordance with legal standards. Information about employees may be disclosed from time to time to the federal agencies that oversee these laws. Workplace injuries may result in the reporting of information to occupational health and safety agencies at both the state and federal levels. Workers' compensation laws direct how injured employees are compensated for their injuries and how they are treated and rehabilitated. The filing of a worker compensation claim will result in the disclosure of information, including health information, to state oversight offices. In addition, state and federal labour laws may impose requirements for the treatment of employee personnel information. These laws seek to maintain a fair balance between employer and worker, and data protection is not a focus of their attention.

8. Executives transferred to the United States become part of the AMFUND Human Resources database just like American employees. The same general policies that apply to the records of American employees apply to records of transferred executives. Some laws that restrict the ability of employers to collect and use personal data apply for the most part only to job applicants. As a result, these legal protections are not applicable to current employees who are just being transferred and who do not qualify as applicants.

9. AMFUND's New York Human Resources office is not aware of any federal or state laws or regulations that restrict the collection of information from employees (other than applicants). A federal law restricts the use of polygraphs in an employment setting, and there are other restrictions on specific collection activities (drug testing and AIDS screening) in some states. New York State law prohibits requesting and using information about arrests and, in some instances, convictions. The lack of awareness of these legal restrictions on workplace information collection may simply be a reflection that the specific data collections are not bank practices. It is highly likely that the same inquiry to the bank's general counsel would result in a complete list of applicable restrictions.

10. The company has an internal 'employee privacy policy' as part of its Human Resources policy manual that establishes data protection standards with general guidance on the collection, use, maintenance, and disclosure of personal data on employees. AMFUND maintains personnel records for payroll, benefit, and incentive purposes, and those requirements (together with external legal requirements) direct the collection, maintenance, and use of employee information. The office also reported that it did not follow any industry code of practice. The International Association for Human Resource Information Management is in the process of preparing a code of practice for employee data based on the Canadian Standards Association Model Code.

11. The real protections bearing on the collection process come from the computer system used to manage Human Resources records. The system has standardised fields for name, address, Social Security Number, company identification number, job and salary history, performance ratings, and the like. If information does not fit into the standard

fields, then it is difficult or impossible to store the information in the Human Resources computer system. For example, the system can store information on job history for up to five prior jobs. Any data on earlier employment cannot be stored in the computer system.

12. AMFUND does not have a written notice that tells employees about the company's information disclosure policies and practices. Thus, when the Congress recently established a federal database for newly hired employees and required most employers to send information to that database, AMFUND did nothing to advise job applicants of the reporting requirement. The federal law does not require that employees be specially notified by employers about the new hire reporting, although some information may be gleaned from the reporting form that an individual may be asked to complete. Information about the federal database appears in the Federal Register, a daily administrative publication for public notices, regulations, and official United States Government agency pronouncements. The requirement for publication of the database description derives from the federal Privacy Act of 1974. That law establishes fair information practices for personal records maintained by federal agencies. The public at large has little awareness of the Federal Register or its contents. When federal agencies collect information directly from individuals, the Privacy Act of 1974 does require that notices be provided on the form or at the time of collection. The notice requirement does not necessarily apply when third parties collect information and provide it to the government.

13. Information from the Human Resources system is routinely disclosed externally (beyond the routinely required government reporting). Information may be disclosed in response to requests for employment verification or for credit-related verification (e.g., application for a mortgage). In these instances, written employee consent is a prerequisite for the disclosure. Governmental requests for employee information may come from the courts and from law enforcement agencies. Some judicial demands for data may result from private civil litigation to which the employee is a party (e.g., divorce or child custody). The company requires that these requests must have a subpoena.

Access, Rectification, and Data Quality

14. Requirements for data accuracy, relevance, timeliness, and completeness are internal to the company. Some information, such as home address and telephone numbers, can be accessed and corrected directly by employees. Employees can also view other information from their own personnel files, including salary, benefits, and other data. Access to these records is regulated by password controls supplemented by a requirement for entry of the employee's Social Security Number.

15. The quality of other information is further maintained by sharing it with employees on a regular basis. At the time of the annual review for merit pay increases, a computer-generated document is printed and sent to each employee. The employee is asked to confirm name, address, identification numbers, job history, and similar data from the personnel records. This annual review affords the data subject an opportunity to confirm or correct the data in the personnel record.

16. In addition, before the enrolment period for company benefits (e.g., open season for switching between company health plans), each employee receives a form that shows demographic and dependent information. The purpose is to make sure that appropriate benefits are available to each employee. This process provides another opportunity for review and correction of employee data.

17. Finally, managers conduct annual personnel reviews with each employee, and the employee signs the resulting review. This affords an opportunity for each employee to discuss the review with his or her manager and to appeal the result if the employee is not satisfied. The Human Resources office receives and maintains the results of that process.

18. Requests for correction of personnel files and appeals of disputes are rare. The employee privacy policy does recognise the right of employees to file notices of disagreement when disputes about information remain unresolved. The company has no policy about notifying third party recipients when a record has been corrected.

Security

19. AMFUND has an information security department that is part of its computer operations division. In addition, each division within the company has its own security officer. For Human Resources records, company policies determine which employees may access which records. A personal profile determines which computer screens an employee may view and which the employee may update.

20. Human Resources files are not encrypted. Audits trails track some file operations. The computer system will record who updated a file although it does not record access without change. However, when an employee requests access to a file that the employee is not entitled to see, the attempt is recorded as a security violation and may result in an investigation.

Onward Transfer Restrictions

21. Except for demands from federal and state governments, personnel files are not routinely transferred to third parties. Employee lists are not made available to direct marketers or others. Under federal labour law, it is possible for some employee information to be disclosed to union officials during labour negotiations. When an employee who was transferred from Europe returns to another job in Europe or in a bank office in another country, the employee's personnel information is returned to London. The London office then forwards the information to the new location. Information is retained onsite in the United States for six months following the transfer of an employee to another location. The information is then archived offsite. This is the standard record retention policy for all personnel files.

Remedies

22. Remedies for employees aggrieved about fair information practices may occasionally be available under specific state or federal laws. For example, the federal law regulating the use of polygraphs by employers provides civil penalties that may be enforced by the Secretary of Labour. Aggrieved employees may also bring private civil actions, with awards of damages, lost wages, reinstatement, and attorney fees available to successful litigants. Other laws, such as the Fair Credit Reporting Act, also include specific administrative enforcement and civil liability provisions.

23. For the most part, however, employees have no simple, direct, or unitary way to enforce fair information practices. Improper collection, use, or disclosure activities by an employer could theoretically give rise to liability under several different state and federal statutes, with possible administrative enforcement and oversight by different government offices. As a practical matter, independent enforcement and oversight of fair information practices are rare.

24. American tort law developed common-law remedies for invasions of privacy. Four distinct privacy torts are commonly recognised: 1) intrusion upon an individual's seclusion or solitude; 2) public disclosure of private facts; 3) placing an individual in a false light highly offensive to a reasonable person; and 4) unpermitted use for private commercial gain of a person's identity. Of the four tort remedies, New York State law only recognises the

fourth. No common-law privacy remedies are available in New York, so the other three privacy torts are unavailable in the state.

25. As a result, a transferred (or other) employee seeking to obtain access to a personnel record or to force a correction to a record would have to find a statutory or contractual basis for a lawsuit. The diversity of applicable statutes might create a cause of action for some elements of fair information practices, but the cost and novelty of a lawsuit would be challenging at best.

26. Even if clear legal remedies were available, they would not likely be directly responsive to privacy concerns reflected in fair information practices. Most elements of fair information practices are not attainable through litigation. For example, the classic privacy torts are not likely to force a record keeper to publish descriptions of record systems, limit collection practices, meet data quality standards, allow individual access and correction, or restrict internal uses of data.

27. Restrictions on the disclosure of personal data may be a possible remedy for the tort of appropriation of name or likeness. For the most part, personal information is used inside organisations in ways that are not visible to the outside world or to the subject of the information. There is no physical intrusion or public disclosure. No false light is shed. By themselves, privacy torts are not likely to offer effective remedies to employees concerned about fair information practices. Whether an AMFUND employee could sue to force the company to comply with its stated privacy policy is uncertain. Unless a contractual obligation or unfair labour practice were found, litigation would be problematic.

28. Aggrieved employees in some states might have other remedies, at least in theory. The right of privacy under the California State Constitution has been held to apply to private conduct, and it might be invoked to support an objection to an employer privacy practice.

29. Whatever statutory or other remedies might be available to employees in the United States or in New York State should, for the most part, be available equally to American citizens and to foreign nationals alike. The federal Privacy Act of 1974 does not give any right to foreign nationals, but it does grant rights aliens lawfully admitted for permanent residence. That Act applies only to personal records maintained by federal agencies and is not directly relevant to employees of AMFUND except if their records come into the possession and control of a federal agency.

Accountability

30. A written employee privacy policy for Human Resources records addresses many of the elements of fair information practices in general terms. The policy document is available to all bank employees. The policy reflects a general policy of limited internal use and limited external disclosure. Employees have a right to access and correct their records. Security is a required element in the policy, and misuse of personal information can result in the dismissal of an employee. The policy also establishes standards for accuracy. Records that are being disposed must be shredded. Each employee in the Human Resources office must sign a non-disclosure agreement.

31. The Senior Vice-President for Human Resources oversees privacy policy for Human Resources records. That person may be the equivalent of a privacy officer.

32. Staff training in the bank's privacy policy is conducted routinely as part of other training activities for Human Resources employees.

33. Bank activities are subject to annual external audits and internal reviews. The bank conducts no reviews specifically focused on compliance with privacy requirements, but

violations of security recorded during routine monitoring may be the subject of further investigation during other reviews.

Conclusions

34. AMFUND policies incorporate most elements of fair information practices. Employees receive notice of privacy policies, and they have the ability to see and correct many, if not most, of their personnel records. The bank has policies addressing limiting both use and external disclosure. The personnel computer system limits the collection and maintenance of some information simply by not having the capacity to store the data. Security protections are in place.

35. Disclosures to government agencies are both routine (e.g., tax withholding) and occasional. Federal agencies receiving employee information are subject to the Privacy Act of 1974. Comparable general purpose privacy laws for state agencies are found only occasionally, although New York is one of the minority of states with a law. Information disclosed to non-governmental organisations (e.g., providers of health plans) is likely to be subject to no statutory fair information practice protections. As with AMFUND, the majority of protections for any private sector record keeper are likely to arise from internal policies rather than from statutes.

36. One major area where clear deficiencies arise is enforcement. An employee seeking to enforce fair information practices through the courts or other independent means bears a heavy burden. No state or federal privacy office exists to provide assistance. Federal or state labour agencies might have some limited jurisdiction over some matters, but processing fair information practice complaints is not a routine activity. For the most part, employees seeking enforcement of fair information practices can only rely on the good faith of their employers or on a court system that is remote, expensive, and offers no well-established precedents.

37. Overall, AMFUND's internal policies offer a reasonable prospect of a good level of compliance with most fair information principles. Federal and state laws and industry codes do not provide much direction to the company or assistance to employees, however. Data subjects requiring assistance to enforce fair information practices will receive some support through AMFUND's standard internal procedures. External assistance from federal or state regulators is likely to be difficult to obtain because there is no office with focused responsibilities. Similarly, internal AMFUND remedies for employees are likely to be useful, but external enforcement remedies through the courts or otherwise will be problematic.

Conclusions about Human Resources Data

1. Compliance with fair information practices for the six Human Resources transfers studied is generally good. In all the cases studied, at least some elements of fair information principles have been incorporated into organisational practices. In most jurisdictions, many of the elements considered necessary for adequacy have been achieved.

2. The reason for this positive showing here is that, in each case, the recipient organisation in the destination jurisdiction is a subsidiary of a European parent company. Because the parent company must already comply with data protection policies through the law of its home country, many of the required practices have been institutionalised and incorporated directly into company policies worldwide. In effect, the parent company exports its 'home country' data protection policies along with its data. If it were common for employees' data to be transferred to an independent organisation wholly unrelated to the parent company, it is unlikely that a similarly good level of compliance would be found in those jurisdictions that do not have comprehensive data protection laws.

3. In some instances, the Human Resources software used actually helps to achieve compliance with some data protection practices. If, for example, the software used by a Human Resources department does not include the capability to store outdated information, then there is no practical way for the data to be maintained. In effect, compliance becomes automatic in these instances.

4. In New Zealand and Hong Kong, which have private-sector data protection laws similar to those in European Union member states, compliance with fair information practices standards appears to be at the highest level. Both New Zealand and Hong Kong offer independent dispute-resolution mechanisms. In jurisdictions without comprehensive data protection laws, external standards for fair information practices are hard to find, and independent dispute resolution mechanisms for data protection are not likely to exist. Some local labour laws and rules offer the possibility of enforcement of some data protection elements, however.

5. In the absence of a specific law on the subject, as is found in Hong Kong but not elsewhere, restrictions on the onward transfer of personal data are dependent on company policies. In the Human Resources area, companies have few, if any, reasons to permit the transfer of employee information to other jurisdictions, except to other subsidiaries of the parent company. The lack of any reason to make such transfers may offer the best assurance of both good policies and good compliance. The development of international Human Resources codes of practice may offer some assistance in the future to adequacy assessors.

Sensitive Data in Airline Reservations

(a) *Australia*

The Nature and Circumstances of the Transfer

1. FLYBEST Airlines is a major international carrier which flies into major cities in Australia. It has employees in offices across Australia, but also contracts with an Australian airline, JETWELL, to provide check-in services at Australian airports. This case study takes a hypothetical journey and identifies the multiple transborder transfers of personal information associated with it, before focusing on the protection afforded to the data that is transferred into Australia.

The Booking

2. A citizen of Eurostate, a country in the European Union (EU), flies economy class from Euroville to Sydney, Australia on a direct FLYBEST flight to Singapore, then on a code-share JETWELL flight to Sydney. After business in Sydney, he flies on to Auckland, New Zealand on the New Zealand airline SOUTHFLIGHT.

3. The passenger is a member of FLYBEST's Managers' Club (which automatically includes the 'frequent-flyer' programme). He will require a wheelchair at all airports and kosher meals on all flights. FLYBEST knows this from his profile when the flight is booked and his Managers' Club number is provided.

4. The booking of a flight can be made directly from the airline either through a FLYBEST office (in person or by telephone) or through FLYBEST's Internet site. Flights can also be booked through a travel agent who will have indirect access via international reservation systems such as Galileo or Sabre. The origin of the booking does have some subtle implications for how personal data are stored and transmitted (see 'Recommendation 1/98 on Airline Computerised Reservation Systems', from the EU's Article 29 Working Party). For this scenario, however, we assume that the booking is made directly through FLYBEST's telephone sales department.

Personal Information Flows - Euroville-to-Sydney Flight

5. When the passenger books his flight in Eurostate, a 'Passenger Name Record' (PNR) is created in FLYBEST's Computerised Reservation System (CRS), the database for which is located in Eurostate. PNRs must contain a name, itinerary, phone number, the ticketing option (i.e., by what date it must be paid for), and the name of the person who phoned in the reservation. The fares and taxes payable are calculated automatically (taking account of any special fares) and the amount and method of payment will also be added in due course - if by credit card, the card type, number, expiry date and merchant authorisation code. In this case, the PNR would also hold the request for a special meal and a wheelchair, recorded as internationally recognised codes which have been issued by the International Air Transport Association (IATA). The disability code used indicates that the passenger needs a wheelchair but is not totally immobile. Permanent preferences registered by Managers' Club members are transferred automatically from the Club database into the CRS. Other codes entered on a one-off basis in these fields of the database would indicate such additional characteristics as unaccompanied minor, deportee, prisoner under escort, etc., or special needs for passengers who are not Club members. Seat allocations are generated in advance for First and Business Class passengers, Club members and others with special needs, while seat allocations for most other economy passengers are currently not made until check-in.

6. Some countries, including Australia, now offer electronic visas to speed up passenger processing at ports of entry (and reduce paperwork in High Commissions).

Passengers who choose to take advantage of this system provide FLYBEST with additional information required by the relevant immigration authorities. This is entered into a module within the CRS and transmitted on-line to the immigration authorities concerned - in this case in Canberra, Australia. The visa application is processed and an 'electronic visa' issued to the passenger through FLYBEST's CRS.

7. The PNR is held on FLYBEST's mainframe computer in Euroville, to which authorised FLYBEST personnel and agents around the world have access. Between 36 and 48 hours before departure, relevant fields from the PNR are transferred to the Departure Control System (DCS). DCS is a subsidiary database held in Eurostate but, like the CRS, accessible worldwide. The day before the flight, the check-in agents will 'edit' the flight list to make sure there is the appropriate weight distribution, to establish fuel requirements, to order meals, and to ascertain that those with special needs have been properly accommodated.

8. When the passenger checks in for the flight at Euroville Airport, the FLYBEST check-in staff would enter his last name to access his record on the DCS. Check-in staff (whether employees or agents) can also access this information by seat number. At a pre-set time before departure (approximately 30 minutes), a complete list of passengers by seat number is printed and given to the cabin crew; any subsequent last-minute changes are notified separately.

9. The records for each flight are purged from the DCS some two hours after the flight has landed. Printed copies of all flight lists are held by FLYBEST at Euroville Airport for 12 months.

10. The PNR itself is purged from the CRS between 24 and 48 hours after the completion of the last leg of each journey. It is, however, retained in a separate database for two years for the purpose of management analysis.

11. The FLYBEST flight attendants know from the passenger list about special needs and will probably welcome the passenger by name. He will be given his kosher meals, probably in advance of the general meals service.

12. At Singapore airport, where the passenger is in transit for only a few hours, he is taken in a wheelchair by a FLYBEST employee or agent to the JETWELL loading gate, his relevant details having been automatically transferred from the FLYBEST CRS to the JETWELL system. The details transferred would only be the relevant stage booking, the immediately prior connecting flight (if any) and any special needs. 'Second' carriers do not have direct access to FLYBEST's CRS and do not need, or receive, the complete journey details, booking contacts or PNR history.

13. On arrival in Sydney on the JETWELL flight, the passenger is met by a JETWELL employee (or contractor) with a wheelchair and taken to baggage claim, through immigration and customs and to the car-hire check-in desk. The car-hire company, and the hotel at which he is staying, have been notified in advance by FLYBEST local staff, responding to an automatically generated request from the CRS. Some hotel and car-hire chains now have an interface to FLYBEST's CRS and would receive the reservation on-line, although this automated transfer would not convey any 'special needs' such as the wheelchair for the passenger.

14. FLYBEST's Managers' Club is sub-contracted - in Australia, to a company called GOODCARE, located in Melbourne. While in Australia, the passenger may contact FLYBEST to confirm his onward flight details and/or seek general assistance. Unlike with some airline clubs, GOODCARE would not be able to change the bookings for the passenger, although they could make a new flight reservation on the CRS using 'frequent-flyer' points and would refer him to FLYBEST if he wanted to do this.

Personal Information Flows - Sydney-to-Auckland Flight

15. On completion of his business in Sydney, the passenger takes an onward flight to Auckland with SOUTHFLIGHT. FLYBEST have no direct or code-share flights to New Zealand. On check-in at Sydney Airport, the passenger finds again that his details, including special needs, have been transferred by FLYBEST, this time to SOUTHFLIGHT's computer system. The wheelchair and kosher meals are ready when required.

Overview of the Regulatory Environment for This Case

16. There is currently no general privacy law in any Australian jurisdiction. The Commonwealth Privacy Act 1988 applies to the private sector only in relation to the provision of consumer credit and to the use of the government issued Tax File Number.

17. Government policy since 1997 has been not to legislate for privacy protection in the private sector generally, but to encourage industry self-regulation. The Privacy Commissioner has been conducting a consultative process to try to devise National Principles (NPPs) which could be used as the basis either for legislation (which now seems likely in the state of Victoria), or for self-regulatory codes. The Commissioner issued a set of Principles in February 1998, covering all of the core areas of privacy, providing rules about collection, use and disclosure, quality, security and access and correction, and designed to be in line with international best practice, although they are still being finalised. Several business groups have committed themselves to incorporate the Commissioner's Principles in voluntary codes of practice, with associated compliance and complaint-handling mechanisms. The Victorian government has also said that it will adopt the Commissioner's principles as the basis of its statutory regime, to be introduced into Parliament later in 1998.

18. While neither FLYBEST, JETWELL or GOODCARE are members of an industry association that proposes to adopt the Commissioner's Principles, they would all be affected by Victorian legislation when holding or using personal information in that State (subject to any constitutional challenge about restraint of interstate commerce).

19. Airlines are members of a major trade association, IATA, which has headquarters in Montreal. International airline policy is co-ordinated by the International Civil Aviation Authority (ICAO), a United Nations-affiliated body located in Montreal. FLYBEST and JETWELL are subject to the 1996 ICAO 'Code of Conduct for the Regulation and Operation of Computer Reservation Systems (CRS)'. Article 11 states that 'air carriers, system vendors, subscribers and other parties involved in air transportation are responsible for safeguarding the privacy of personal data included in the CRSs to which they have access, and may not release such data without the consent of the passenger.' The ICAO issues standards and recommended practices for both airlines and members states, but it has no enforcement powers.

Purpose Limitation, Transparency and Opposition

Collection

20. Most of the information recorded by FLYBEST in a PNR is either provided by or on behalf of the passenger or is generated by FLYBEST (e.g., the flight and seat numbers). The only information obtained from third parties would be the 'approvals' returned by the immigration authorities in destination countries offering electronic visas, authorisations for credit-card debits, and the reference numbers returned from the CRSs of any other carriers involved in the journey.

21. The FLYBEST Airlines 'Conditions of Carriage' declares that:

> 'The Passenger recognises that personal data has been given to Carrier for the purposes of making a reservation for carriage, for obtaining ancillary services, and for facilitating immigration and entry requirements. For these purposes, the Passenger authorises Carrier to retain such data and to transmit it to its own offices, other carriers or the providers of such services, in whatever country they may be located.'

It is not clear how, and in what manner, this assurance is made known to passengers.

22. In Eurostate, and while the PNR is being accessed by FLYBEST personnel in Australia, the collection and use of personal data will be in accordance with policies set by Head Office in Eurostate. Company policy, worldwide, is guided by the requirements of the Eurostate data protection law. FLYBEST's regional management are aware that there is no equivalent law in Australia, although this would not be widely known to other staff - some would assume that the company policy is a legal requirement. In practice, although not in law, limits imposed on the use of personal data in third countries, for all passengers, are determined by the requirements of the Eurostate data protection law, as interpreted by company policy and communicated to employees.

Use and disclosure for FLYBESTs purposes

23. The information FLYBEST holds about passengers is used by them, and by other organisations involved in the journey, for the purposes of providing travel and related services. These uses are not only within the reasonable expectation of the passenger but will generally be with at least their implied consent. Depending on whether the conditions of carriage cited above are drawn to their attention, this could be taken to be express consent. While FLYBEST itself is subject to the Eurostate data protection law, JETWELL and the Australian hotel and car-hire firms which necessarily receive personal information about the passenger are under no statutory obligation not to use that information for other purposes.

24. Recall also that the passenger is a member of FLYBEST's Managers' Club. There is a separate database of Managers' Club members in each country or region. Most other airlines retain central databases. The Australian database on FLYBEST’s Managers' Club members in Australia and New Zealand is held in Melbourne and managed by GOODCARE, a company on contract (indirectly via a European prime contractor) to FLYBEST. This database holds a profile of the passenger’s flight history, hotel reservation and car-hire needs, frequent-flyer account, and other information (more extensive than the data held in the CRS). There is a daily comparison and update of data between the Australian and New Zealand Managers' Club database and FLYBEST's Customer and Marketing database held in Eurostate. Because there is currently no privacy law applying to general private-sector activities in Australia, the only limits on the use of data either on Managers' Club members, or on other passengers, by GOODCARE are those in the company's own policy and in the terms of their contract with FLYBEST.

25. GOODCARE staff have read-only access to FLYBEST's CRS; they are not able to make changes. FLYBEST personnel will have limited access to Managers' Club data to provide the 'personalised' service that such customers expect. GOODCARE is subject to strict contractual terms but only FLYBEST, as the client, could take action for breach of those terms. A passenger whose information was misused would not be able to take legal action, except perhaps indirectly against FLYBEST.

Disclosure to third parties for other purposes

26. FLYBEST employees in Australia will have been made aware through induction training, and through a notice on the computer-access applications (see below), of the

general policy about the disclosure of reservations information. They are reminded that: 'The carriage by air of passengers is a matter of private contract between the airline and the passenger concerned. As a general rule details of that contract should not be given to third parties particularly when the request is made on the telephone.' Employees are told not to disclose information about a passenger, including via the telephone, unless the information is given to:

- a colleague/another airline or agent for the purpose of reservation booking or ticket issue;
- the passenger himself and you have taken the necessary steps to ensure that this person is the passenger;
- some other person and the passenger has clearly consented to this and there is a record of this in the PNR;
- an appropriate person or organisation in an emergency to prevent injury or damage to someone's health.

27. Employees are also advised, orally, that requests from the police or law enforcement bodies must be referred to the investigations unit, and those relating to legal proceedings to the legal department. They are also advised that details of medical conditions must not be disclosed without reference to the Senior Medical Officer.

28. FLYBEST's personnel work, however, in a number of different settings that might guide the ways in which these rules are interpreted. In a telephone-sales context, they are quite strictly adhered to. If the person to whom the sales agent is speaking is not travelling, or is not mentioned in the contact field of the booking (such as the name of the secretary), then details cannot be given out.

29. In the airport environment, however, practices may differ. FLYBEST staff and agents will have access to passenger information before, during and after a flight. A greater variety of more urgent requests arise within the airport context. In an Australian airport, such requests might come from the federal police (who have jurisdiction over major airports), from State law enforcement authorities, or from Customs and Immigration officials.

30. Requests for personal information from authorities, whether at the airport or to FLYBEST offices, will normally be handled by a supervisor. At the airport, requests from customs or police officers (usually known personally) are handled informally with no record being kept, unless there is a need for an accompanying 'statement' from an employee. JETWELL employees at the airport are expected to refer requests to FLYBEST supervisors, even though the contract, which is the standard IATA contract for ground handling services, does not contain any specific contract terms about confidentiality, (there are such terms in GOODCARE's contract). Current policy in FLYBEST offices is to ask for identification, and usually a faxed request, but not to enquire any further into the justification, or to try to impose any conditions on use or further disclosure. Request forms are filed but no indication is made on the PNR or Club database. The practice of other contractors, including GOODCARE, is not known by FLYBEST, although there is an expectation that they will have similar safeguards. The policies of other carriers such as SOUTHFLIGHT are also not known to FLYBEST, who rely on the passenger's consent for transfer of personal information to other carriers as required (see standard terms above). However, SOUTHFLIGHT, as a New Zealand business, is bound by the New Zealand Privacy Act 1993, which includes both privacy standards and enforcement and complaint mechanisms.

31. The major circumstances under which a passenger's records would be accessed after a flight would be if he left a possession by the seat. If the flight attendant or cleaning crew found a possession, FLYBEST would be able to access the PNR by seat number and contact the telephone number on the PNR (up to the time the PNR is deleted, after which the problem would be handled via Eurostate). JETWELL and SOUTHFLIGHT could be expected to have similar arrangements.

32. The deletion of passenger records from the computer system shortly after the completion of a flight should ensure that PNR data will not be available in Australia (and therefore potentially open to misuse or third-party requests) for any length of time. If there are special requests from third parties after the PNR has been archived, they would have to be made in writing and considered in Eurostate under the data protection law.

Data Quality and Proportionality

33. Given the centralised control of FLYBEST's personal-information policy and computer-systems design, any data that are collected in Australia are largely governed, indirectly, by the requirements of the Eurostate data protection law. Data are collected in order to fulfil the private contract between the carrier and the passenger concerned. The standard minimum amount of information needed for the creation of a PNR would seem necessary and not excessive to fulfil FLYBEST's obligations; any further information supplied (about special needs) is presumably provided by or with the consent of the passenger.

34. Some of this information can, however, be very sensitive. Airlines may collect a variety of medical information: physical handicaps, diabetic status, allergic reactions, etc. Some passengers have special dietary needs: kosher meals, no salt, vegetarian, etc., which give clues to religious affiliation or medical conditions. International airlines might also receive other categories of sensitive data, including information on dignitaries, deportees, unaccompanied minors (who might be in the middle of a parental-custody dispute), and members of groups who have sensitive affiliations, such as some political movements. Some sensitive information is held permanently in the regional Managers' Club databases and this is reconciled daily with FLYBEST's master Customer and Marketing database in Eurostate. Data-quality problems arise from this need for matching, although this will be reduced by the proposed introduction of a new uniform database serving both FLYBEST itself and its Managers' Club contractors.

35. FLYBEST employees are also advised, orally in induction training, to refrain from placing into the central database 'any information or statement about a passenger which may be inaccurate or disparaging or discredit the passenger in any way.' There appears to be no express 'passing on' of this guidance to JETWELL employees acting as FLYBEST's agents, but JETWELL itself can be expected to have a similar policy and training in respect of their own passengers.

Security

36. Security requirements are also directed from Eurostate. None of the PNR data is encrypted. FLYBEST's CRS, the DCS and the Customer and Marketing database are password-protected for all users - its own staff, check-in agents, and GOODCARE staff. There are different levels of access depending on status in the organisation. Employees, agents and contractors' staff needing access all have to complete an application form which also serves to remind them about the need for confidentiality. After endorsement by a supervisor as to the level of access required, the applications are processed in Eurostate and authorisation codes (user IDs) are issued. To access the system, users have to input their ID and a self-selected password (which has to be changed at regular intervals). The history of any changes to a PNR is recorded. There is an audit trail of all access to the CRS.

37. GOODCARE is required by the terms of its contract to maintain a separate operation with dedicated 'front line' staff - i.e., staff cannot service both FLYBEST Managers' Club members and other customers of other clients. GOODCARE's staff have limited (mainly read-only) access to FLYBEST's systems, although GOODCARE's regional membership data are uploaded and reconciled daily with the FLYBEST Customer and Marketing

system. GOODCARE's separate database of regional Club members is protected in similar ways to the FLYBEST systems.

Access and Rectification

38. Access by passengers to personal information held about them by FLYBEST tends to occur for very practical and mundane reasons (such as checking schedules and preferences), and will normally take place prior to departure. These data can also be accessed formally via the 'subject access' provisions of the Eurostate data protection law, which enables European passengers to check the accuracy, relevance and completeness of information. It is difficult to envisage circumstances under which European passengers would want formally to access or correct their records during the very brief period while they are processed by FLYBEST within Australia.

39. If, however, information is lawfully given by FLYBEST to a third party and is retained within Australia for other purposes, the availability of access and correction rights would depend on the jurisdiction. If the information were held by a government agency, these rights would be available under federal or state Freedom of Information laws, (everywhere except the Northern Territory) subject to a range of exceptions. If the information were held in the private or non-government sector, it would only be accessible as of legal right if it were health information held in the Australian Capital Territory. Other private sector organisations may choose to grant access as a matter of company policy or in accordance with one of a number of sectoral codes of practice, but these would not be legally enforceable rights. There may be remedies available under some of the voluntary sectoral schemes but these would vary in scope and effectiveness.

Onward Transfer Restrictions

40. Through its CRS, FLYBEST routinely transfers personal information in PNR records between jurisdictions. The Eurostate data protection law does contain transfer prohibition provisions which can be invoked if there is a perceived risk of a breach of privacy principles as a result of such a transfer. These provisions have recently been amended to bring them into line with the Directive. The issue for this case study is, however, somewhat different. In assessing adequacy of protection in a third county, the Article 29 Working Party has suggested that one important consideration is the availability of controls on the onward transfer of data to jurisdictions with lesser or no privacy protection. Currently in Australia, no organisations holding personal data are subject to express statutory provisions about onward transfer. Those federal government agencies subject to the Privacy Act are however required to comply with a security principle which includes a requirement:

> 'that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.' (Information Principle 4 (b), Section 14, Privacy Act 1988 (Cwth))

41. This could arguably be invoked to prevent a federal government agency knowingly transferring data outside Australia (or outside the Commonwealth jurisdiction) without taking steps to protect the data, such as imposing appropriate terms and conditions in any contract. However, this provision could not be used to ensure compliance by the recipient with any of the other principles, and only applies to the provision of services, not to the release of information for a third party's own purposes.

42. The Privacy Commissioner's National Principles do contain a Transborder Data Flow Principle, and if adopted in law or in binding codes, this could close the current

loophole provided by the absence of any onward-transfer restriction outside the limited scope of the Privacy Act IPP 4(b) provision.

Remedies

43. FLYBEST has an internal complaints-handling process. Most complaints relate to issues such as pricing and the flexibility of the tickets purchased, as well as to the flight experience. Complaints about breaches of the privacy principles are rare, and have never been recorded in Australia. Before the flight, complaints are handled through a hierarchy of service agents, managers and directors. If the complaint occurs after the flight is taken, it will be referred to the most appropriate branch of the Customer Relations Department**.**

44. There is no Australian authority outside the organisation to which complaints about privacy intrusion by an international airline passenger might be referred. There are no external remedies available in Australia for passengers alleging a breach of any of the 'standard' privacy principles - collection, use limitation, data quality, access and correction, and security - by any of the parties involved. FLYBEST passengers from Eurostate could exercise their rights under the Eurostate data protection law in relation to actions by FLYBEST itself, but there would clearly be practical difficulties in investigating and resolving complaints about actions that had taken place in Australia, especially if they involved JETWELL, SOUTHFLIGHT or GOODCARE.

Accountability

45. Theoretically, FLYBEST's employees, agents and sub-contractors in Australia should be given exactly the same guidance about personal-information practices as their counterparts in Eurostate. Written policies, already cited, are available online and drawn to staff's attention during induction. There is no privacy officer, designated as such, in FLYBEST's regional organisational structure, but security personnel assume broad responsibility for monitoring access to the central reservation system.

46. Because it is subject to the Eurostate data protection law, FLYBEST is accountable for its personal information handling practices to the Data Protection Authority, which has a range of powers to ensure compliance if breaches of privacy or weaknesses in an organisation's systems are brought to its attention, although it does not have the power to conduct pro-active audits of compliance.

47. FLYBEST is only subject to the Eurostate law in respect of data held (controlled) outside Eurostate if those data are intended to be used in Eurostate. In the circumstances of this case study, it seems clear that any data held on FLYBEST's main computer systems would be subject to the Eurostate law, although it is arguable whether data about an international passenger held locally by FLYBEST staff in Australia would be covered. However, since FLYBEST chooses to apply the standards required by Eurostate law to all its operations worldwide, data held and processed in a third country, such as Australia in this case study, benefit from the overall protection and accountability, even where it has no legal force.

Conclusions

49. For airlines like FLYBEST, guided by established set of data protection standards within their 'home country' legislation, there should be little difference between practices in Australia (or in any other third country) and those in the home country, in this case, Eurostate. Only systematic on-site auditing can, of course, determine whether or not company policy and guidance is followed.

50. For Australian carriers such as JETWELL, it is probable that rules about handling of personal information are less stringent and less carefully followed. However, the available evidence cannot indicate the precise ways in which practices differ from those of their European counterparts. SOUTHFLIGHT, a New Zealand airline, is subject to the New Zealand Privacy Act 1993. The scope, content and overall 'adequacy' of the New Zealand law is considered in the case studies of primary transfers to New Zealand elsewhere in this Report, and is not considered further in this case study.

51. There is currently no Australian data protection supervisory authority, either at State or federal level, with jurisdiction over the personal information held by airlines, whether domestic or international except if they hold credit information or Tax File Numbers in Australia.

52. If passenger data are revealed to third parties, then a range of federal and state laws may apply to provide some privacy protection. Federal agencies, including Customs, Immigration and the Federal Police, are regulated by the Commonwealth Privacy Act of 1988, which requires compliance with a comprehensive set of data protection principles and has effective complaint and enforcement mechanisms. Some State agencies are subject to statutory secrecy and confidentiality provisions, and in some States all government agencies are required to follow modified sets of privacy principles by administrative direction (not law). The need for privacy law is currently being debated both at federal level and in some of the States, as outlined above.

53. The potential for breaches of the privacy of a passenger with a European airline passing through Australia are probably quite limited, largely because of the integrity and security of airline systems and the fact that much of the personal information held never passes outside the airline. While held by the airline, the data protection law of the airline's home country will provide the same protection for passengers as if they were travelling in Europe, although there may be practical difficulties in investigating and enforcing compliance by the airline's locally based staff.

54. To the extent that data do leave the control of the airline - passing to local agents, code-share partners or third parties - there is no statutory privacy protection, no effective applicable codes of practice, and apparently only limited contractual safeguards. European passengers would have no effective remedies if one of these third parties breached their privacy.

Sensitive Data in Airline Reservations

(b) *Canada*

The Nature and Circumstances of the Transfer

1. TRANSGLOBE Airlines is a major international carrier which operates direct flights from Europe to Montreal, Vancouver and Toronto. It has about 200 employees in offices across Canada.

The Booking

2. A citizen of Eurostate, a country in the European Union (EU), flies economy class from Euroville to Montreal, Quebec on a direct TRANSGLOBE flight, then on a code-share TRANSCAN flight to Vancouver, British Columbia.

3. The passenger is a member of TRANSGLOBE's Managers' Club (which automatically includes the 'frequent flyer' programme). He will require a wheelchair at all airports and kosher meals on all flights. TRANSGLOBE knows this from his profile when the flight is booked and his Managers' Club number is provided.

4. The booking of a flight directly from the airline is one of four ways that international bookings might take place. Thus our passenger could also reserve the flight through a travel agent who will have access to international reservation systems such as Galileo or Sabre. He might reserve through TRANSGLOBE's Internet site. He might call the toll-free number associated with TRANSGLOBE's frequent flyer programme. The origin of the booking does have some subtle implications for how personal data are stored and transmitted (see 'Recommendation 1/98 on Airline Computerised Reservation Systems', from the EU's Article 29 Working Party). For this scenario, however, we assume that the booking is made directly through TRANSGLOBE's telephone sales department.

Personal Information Flows - Euroville-to-Montreal Flight

5. When the passenger books his flight in Eurostate, a 'Passenger Name Record' (PNR) is created in TRANSGLOBE's Computerised Reservation System (CRS), the database for which is located in Eurostate. PNRs must contain a name, itinerary, phone number, the ticketing option (i.e., by what date it must be paid for), and the name of the person who phoned in the reservation. The fares and taxes payable are calculated automatically (taking account of any special fares) and the amount and method of payment will also be added in due course - if by credit card, the card type, number, expiry date and merchant authorisation code. In this passenger's case, the PNR would also hold the request for a special meal and a wheelchair, accessible by internationally recognised codes which have been issued by the International Air Traffic Authority (IATA). The disability code used indicates that the passenger needs a wheelchair but is not totally immobile. Permanent preferences registered by Managers' Club members are transferred automatically from the Club database into the CRS. Other codes entered on a one-off basis in these fields of the database would indicate such additional characteristics as unaccompanied minor, deportee, prisoner under escort, etc., or special needs for passengers who are not Club members. Seat allocations are generated in advance for First and Business Class passengers, Club members and others with special needs, while seat allocations for most other economy passengers are currently not made until check-in.

6. The PNR is held on TRANSGLOBE's mainframe computer in Euroville, to which authorised TRANSGLOBE personnel around the world have access. Between 36 and 48 hours before departure, relevant fields from the PNR are transferred to the Departure

Control System (DCS). DCS is a subsidiary database held in Eurostate but, like the CRS, accessible worldwide. The day before the flight, the check-in agents will 'edit' the flight list to make sure there is the appropriate weight distribution, to establish fuel requirements, to order meals, and to ascertain that those with special needs have been properly accommodated.

7. When the passenger checks in for the flight at Euroville Airport, the TRANSGLOBE check-in staff would enter his last name to access his record on the DCS. Check-in staff (whether employees or agents) can also access this information by seat number. At a pre-set time before departure (approximately 30 minutes) a complete list of passengers by seat number is printed and given to the cabin crew; any subsequent last minute changes are notified separately.

8. The records for each flight are purged from the DCS some two hours after the flight has landed. Printed copies of all flight lists are held at Euroville Airport for 12 months.

9. The PNR itself is purged from the CRS between 24 and 48 hours after the completion of the last leg of each journey. It is, however, retained in a separate database for two years for the purpose of management analysis.

10. The TRANSGLOBE flight attendants know from the passenger list about special needs and will probably welcome the passenger by name. He will be given his kosher meals, probably in advance of the general meals service.

11. On the flight, he is asked to fill in a 'Welcome to Canada' card issued by Canada Customs and Immigration. He is required to provide the following information: name, permanent address, date and place of birth, nationality, passport number, flight number, purpose of visit and the value of all goods being brought to Canada as gifts. On arrival, the passenger will be met by TRANSGLOBE's special services and will be taken to baggage claim and through immigration and customs. Here he will surrender his 'Welcome to Canada' card to Canada Customs which, some weeks later, will be processed and entered into the Canada Customs information system. Airline personnel will not have access to the information provided on these cards. These data will be protected under the federal Privacy Act of 1982, overseen by the Federal Privacy Commissioner.[3]

Personal Information Flows - Montreal-to-Vancouver Flight

12. The passenger stays in Montreal for three days before taking an onward flight via TRANSCAN to Vancouver. TRANSGLOBE has a code-share arrangement with TRANSCAN. The onward flight appears as a TRANSGLOBE-coded flight on the passenger's ticket. The details transferred would only be the relevant stage booking, the immediately-prior connecting flight and any special needs. 'Second' carriers do not have direct access to TRANSGLOBE's CRS and do not need, or receive, the complete journey details, booking contacts or PNR history.

13. On arrival in Vancouver, the passenger leaves the airport by a hired car and proceeds to a hotel. The car company and the hotel can receive reservations directly through the TRANSCAN CRS, although the transfer of data would not convey special-needs information such as the use of a wheelchair.

[3] The Privacy Commissioner is currently challenging the constitutionality under the search and seizure provisions of the *Canadian Charter of Rights and Freedoms* of a data matching arrangement between Canada Customs and Human Resources Development Canada (HRDC) for the comparison of these customs data with unemployment insurance records. At issue is HRDC's practice of collecting data from the Customs declarations of every returning traveller to identify employment insurance claimants (supposedly available for work) who were out of the country while receiving benefits.

Overview of the Regulatory Environment for this Case

14. Quebec is the only jurisdiction in North America with a data protection statute similar in scope and intent to those in the European Union. The typical range of information privacy principles is included within the Act Respecting the Protection of Personal Information in the Private Sector (Bill 68). This legislation is overseen by the *Commission d'Accès à l'Information* (CAI), which has a investigative, regulatory and advisory responsibilities for both public and private sectors in the province of Quebec.

15. There is considerable doubt, however, as to whether the jurisdiction of the CAI extends to organisations within the transportation sector, which fall under the jurisdiction of the federal government. The Quebec CAI would like jurisdiction, but their current court challenge against a major Canadian airline over a case involving the misuse of an employee's medical records has already failed at the Superior Court level. The CAI would have jurisdiction, however, if the data were disclosed outside the airline to law enforcement agencies, or to private-sector organisations such as car-hire companies, hotels, contractors, insurance companies, travel agencies or direct-marketing enterprises. No such case has yet arisen since Bill 68 has been in existence. The recently tabled federal Personal Information Protection and Electronic Documents Act (Bill C-54) will, however, apply to federally regulated industries, such as the airlines."

16. In other provinces, including British Columbia (the destination of the onward flight), no data protection legislation or independent supervisory authority would have jurisdiction over TRANSGLOBE's operations, nor over any disclosures to private-sector organisations, such as the car-hire company or the hotel. The public sector Freedom of Information and Protection of Privacy Act would apply in the unlikely event that passenger information were transferred to provincial public body. If passenger information were obtained by federal agencies, the federal Privacy Act would apply.

17. TRANSGLOBE is a member of the Canadian Direct Marketing Association (CDMA), and is therefore expected to comply with the CDMA's code of practice when it uses passenger information for marketing purposes. However, TRANSCAN is not a member.

18. Airlines are members of a major trade association, IATA, which has headquarters in Montreal. International airline policy is co-ordinated by the International Civil Aviation Authority (ICAO), a United Nations-affiliated body located in Montreal. TRANSGLOBE and TRANSCAN are subject to the 1996 ICAO 'Code of Conduct for the Regulation and Operation of Computer Reservation Systems (CRS)'. Article 11 states that 'air carriers, system vendors, subscribers and other parties involved in air transportation are responsible for safeguarding the privacy of personal data included in the CRSs to which they have access, and may not release such data without the consent of the passenger.' The ICAO issues standards and recommended practices for both airlines and members states, but it has no enforcement powers.

Purpose Limitation, Transparency and Opposition

Collection

19. Most of the information recorded by TRANSGLOBE in a PNR is either provided by or on behalf of the passenger, or is generated by TRANSGLOBE (e.g., the flight and seat numbers). The only information obtained from third parties would be authorisations for credit-card debits and the reference numbers returned from the CRSs of any other carriers involved in the journey.

20. The TRANSGLOBE 'Conditions of Carriage' declares that:

‘The Passenger recognises that personal data has been given to Carrier for the purposes of making a reservation for carriage, for obtaining ancillary services, and for facilitating immigration and entry requirements. For these purposes, the Passenger authorises Carrier to retain such data and to transmit it to its own offices, other carriers or the providers of such services, in whatever country they may be located.'

It is not clear how, and in what manner, this assurance is made known to passengers.

21. In Eurostate, and while the PNR is being accessed by TRANSGLOBE personnel in Canada, the collection and use of personal data will be in accordance with policies set by Head Office in Eurostate. Company policy, worldwide, is guided by the requirements of the Eurostate data protection law. TRANSGLOBE representatives claim that the company's data protection policies are probably somewhat tighter than those of airlines operating in Canada. For a passenger originating in Eurostate, therefore, limits imposed for the collection of personal data are determined by the requirements of Eurostate data protection law, as interpreted by company policy and communicated to employees.

Use and Disclosure for TRANSGLOBE's Purposes

22. The information TRANSGLOBE holds about passengers is used by them, and by other organisations involved in the journey, for the purposes of providing travel and related services. These uses are not only within the reasonable expectation of the passenger but will generally be with at least their implied consent. Depending on whether the Conditions of Carriage cited above are drawn to their attention, this could be taken to be express consent. While TRANSGLOBE itself is subject to Eurostate data protection law, TRANSCAN and the Canadian hotel and car-hire firms that necessarily receive personal information are under no statutory obligation not to use that information for other purposes.

23. Recall also that the passenger is a member of TRANSGLOBE’s Managers' Club. This database holds a more complete profile of the passenger’s flight history, hotel reservation and car-hire needs, frequent-flyer history, and other information. TRANSGLOBE personnel have complete access to these data to provide the 'personalised' service that such customers have come to expect. It should be noted, however, that TRANSGLOBE retains a separate database of its frequent-flyer passengers (including those receiving special services) in each country or region. Most other airlines retain central databases. Thus, the Canadian database on TRANSGLOBE’s frequent flyers, held in Toronto and managed by a United States marketing company, will only have information on Canadian members. It is unlikely that data on a European passenger would find its way to this database.

24. The application form for the TRANSGLOBE frequent-flyer programme is presumably quite standard, however. The Canadian version states: 'The information requested on this application, together with the records we will retain relating to your air travel and participation...are to help us better serve your needs. This information is kept confidential at our TRANSGLOBE Service Centre but may be disclosed to partners or other companies who provide benefits and services to TRANSGLOBE members. Please check if: a) You do not wish the above personal information disclosed to partners or other companies; and b) You do not wish to receive separate communications about new services and facilities developed by TRANSGLOBE and its partners.'

Disclosure to third parties for other purposes

25. TRANSGLOBE employees in Canada will have been made aware through training, and through a notice in the computer-access applications (see below) of the general policy about the disclosure of reservations information. They are reminded that: 'The carriage by air of passengers is a matter of private contract between the airline and the passenger

concerned. As a general rule details of that contract should not be given to third parties particularly when the request is made on the telephone.' Employees are told not to disclose information about a passenger, including via the telephone, unless the information is given to:

- a colleague/another airline or agent for the purpose of reservation booking or ticket issue;
- the passenger himself and you have taken the necessary steps to ensure that this person is the passenger;
- some other person and the passenger has clearly consented to this and there is a record of this in the PNR;
- an appropriate person or organisation in an emergency to prevent injury or damage to someone's health.

26. Employees are also advised orally that requests from the police or law-enforcement bodies must be referred to the investigations unit, and those relating to legal proceedings to the legal department. They are also advised that details of medical conditions must not be disclosed without reference to the Senior Medical Officer.

27. TRANSGLOBE personnel work, however, in a number of different settings that might guide the ways in which these rules are interpreted. In a telephone-sales context, they are quite strictly adhered to. If the person to whom the sales agent is speaking is not travelling, or is not mentioned in the contact field of the booking (such as the name of the secretary), then details cannot be given out.

28. In the airport environment, however, practices may differ. TRANSGLOBE staff and agents will have access to PNRs both before, during and after a flight. A greater variety of more urgent requests arise within the airport context, in which such requests might come from local law-enforcement authorities (who have jurisdiction over most airports), from the federal Royal Canadian Mounted Police (RCMP), or from Customs and Immigration officials. Working within a closer environment, personal contacts obviously develop between individuals from different authorities. TRANSGLOBE representatives acknowledge that these personal relationships can often override the formal written guidance, although under most circumstances requests for information have to be in writing and referred to Eurostate.

29. The major circumstances under which the passenger's records would be accessed after a flight would be if he left a possession by the seat. If the flight attendant or cleaning crew found a possession, TRANSGLOBE staff would be able to access the PNR by seat number and contact the telephone number on the PNR. This would only be possible up to the time the PNR is deleted, after which the problem is handled via Eurostate.

30. The deletion of passenger records from the computer system shortly after the completion of a flight should ensure that PNR data will not be available in Canada (and therefore potentially open to misuse or third-party requests) for any length of time. If there are special requests from third parties after the PNR has been archived, they would have to be made in writing and considered in Eurostate under the data protection law.

Data Quality and Proportionality

31. Given the central direction of TRANSGLOBE's personal-information policy and computer-systems design, any data that are collected are largely governed, indirectly, by the requirements of the Eurostate data protection law. Data are collected in order to fulfil the private contract between the carrier and the passenger concerned. The standard minimum amount of information needed for the creation of a PNR would seem necessary and not excessive to fulfil TRANSGLOBE's obligations; any further information supplied (about special needs) is presumably provided by or with the consent of the passenger.

32. Some of this information can, however, be very sensitive. Airlines may collect a variety of medical information: physical handicaps, diabetic status, allergic reactions, etc. Some passengers have special dietary needs: kosher meals, no salt, vegetarian, etc., which give clues to religious affiliation or medical conditions. International airlines might receive other categories of sensitive data, including information on dignitaries, deportees, unaccompanied minors (who might be in the middle of a parental-custody dispute), and members of groups who have certain sensitive affiliations, such as some political movements.

33. TRANSGLOBE employees are also advised to refrain from placing into the central database 'any information or statement about a passenger which may be inaccurate or disparaging or discredit the passenger in any way.'

Security

34. Security requirements are also directed from Eurostate. None of the PNR data is encrypted. TRANSGLOBE's CRS, the DCS and the Customer and Marketing database are password-protected for all users - its own staff and check-in agents. There are different levels of access depending on status in the organisation. Employees, agents and contractors' staff needing access all have to complete an application form which also serves to remind them about the need for confidentiality. After endorsement by a supervisor as to the level of access required, the applications are processed in Eurostate and authorisation codes (user IDs) are issued. To access the system, users have to input their ID and a self-selected password (which has to be changed at regular intervals). The history of any changes to a PNR is recorded. There is an audit trail of all access to the CRS.

Access and Rectification

35. Access by passengers to personal information held about them by TRANSGLOBE tends to occur for practical and mundane reasons (such as checking schedules and preferences), and will normally take place before departure. These data can also be accessed formally via the 'subject access' provisions of the Eurostate data protection law, which enables European passengers to check the accuracy, relevance and completeness of information. It is difficult to envisage circumstances under which European passengers would want formally to access or correct their records during the very brief period while they are processed by TRANSGLOBE within Canada.

36. If, however, information is lawfully given by TRANSGLOBE to a third party and is retained within Canada for far longer, the passenger's exercise of access and correction rights would depend upon the circumstances. If the data were provided to a federal government agency (such as Canada Customs), the federal Privacy Act might be invoked. Rights of access under this legislation, however, can only be exercised by Canadian citizens or permanent residents (Privacy Act, Section 12 (1)). Foreign nationals would, however, be able to lodge a complaint to the federal Privacy Commissioner, assuming they could point to an abuse of the information by the federal agency; TRANSGLOBE airlines itself does not currently come under the Privacy Commissioner’s jurisdiction.

37. Suppose, now, that a disclosure was made about this European passenger to local law-enforcement officials in Montreal. These agencies fall under the jurisdiction of the CAI of Quebec and the public-sector legislation, 'Respecting Access to Documents held by Public Bodies and the Protection of Personal Information' (R.S.Q., Chapter A-2.1). Therefore, the passenger could obtain access to personal information, subject to payment of a fee for transcription and reproduction, and provided the information is not held in a confidential file. The passenger would also be able to lodge a complaint with the CAI.

There are no restrictions as to nationality or residency for the exercise of these rights under Quebec law.

Onward Transfer Restrictions

38. TRANSGLOBE does not transfer personal information from PNR records to officials within other jurisdictions. If, for example, United States law-enforcement authorities were interested in a passenger list, they would have to apply in writing to TRANSGLOBE's Eurostate officials.

39. Although its jurisdiction over the airline industry is questionable, Quebec's Bill 68 contains the only provision in Canadian law relating to onward transfers of data. Section 17 says:

> 'Every person carrying on an enterprise in Quebec who communicates, outside Quebec, information relating to persons residing in Quebec or entrusts a person outside Quebec with the task of holding, using or communicating such information on his behalf must take all reasonable steps to ensure
>
> > (1) that the information will not be used for purposes not relevant to the object of the file or communicated to third persons without the consent of the persons concerned...
> > (2) In the case of nominative lists, that the persons concerned have a valid opportunity to refuse that personal information concerning them be used for purposes or commercial or philanthropic prospection and, if need be, to have such information deleted from the list.'

40. These provisions have yet to be tested, and they only apply to Quebec residents or citizens. However, they signal a possible approach to the regulation of onward transfers from Canada. The approach places a strict liability on the domestic enterprise for the protection of personal data, wherever it is processed. A Quebec resident, under this arrangement, could have a remedy under Quebec law against a Quebec company if it disclosed personal information to a third party in another jurisdiction.

Remedies

41. TRANSGLOBE has an internal complaints-handling process. Most complaints relate to issues such as pricing and the flexibility of the tickets purchased, and tend to arise before the flight is taken. Complaints about breaches of the privacy principles are rare. Before the flight, complaints are handled through a hierarchy of service agents, managers and directors. If the complaint occurs after the flight is taken, it will be referred to the most appropriate branch of the Customer Relations Department.

42. In Quebec, the CAI has received and investigated complaints from employees about airline practices (Canadian and non-Canadian), even though the CAI's authority is still somewhat unclear. In no other province would any Privacy Commissioner have jurisdiction over an airline, whether domestic or foreign. If and when Bill C-54 is passed, individuals will have a right of redress against airlines through the Federal Privacy Commissioner, and ultimately through the federal courts, for any breaches of the privacy principles.

Accountability

43. Theoretically, TRANSGLOBE's employees, agents and sub-contractors in Canada should be given exactly the same guidance about personal-information practices as their counterparts in Eurostate. Written policies, already cited, are disseminated in paper format

and online. There is no privacy officer, designated as such, but security personnel assume broad responsibility for monitoring access to the central reservation system.

44. Because it is subject to the Eurostate data protection law, TRANSGLOBE is accountable for its personal information handling practices to the Data Protection Authority, which has a range of powers to ensure compliance if breaches of privacy or weaknesses in an organisation's systems are brought to its attention, although it does not have the power to conduct pro-active audits of compliance.

45. TRANSGLOBE is only subject to the Eurostate law in respect of data held (controlled) outside Eurostate if those data are intended to be used in Eurostate. In the circumstances of this case study, it seems clear that any data held on TRANSGLOBE's main computer systems would be subject to the Eurostate law, although it is arguable whether data about an international passenger held locally by TRANSGLOBE staff in Canada would be covered. However, since TRANSGLOBE chooses to apply the standards required by Eurostate law to all its operations worldwide, data held and processed in a third country, such as Canada in this case study, benefit from the overall protection and accountability, even where it has no legal force.

Conclusions

46. For airlines like TRANSGLOBE, guided by a more established set of data protection standards within their 'home country' legislation, there should be little difference between practices in Canada (or in any other third country) and those in the home country, in this case, Eurostate. Only systematic on-site auditing can, of course, determine whether or not guidance is followed. For domestic carriers like TRANSCAN, it is probable that the rules are less stringent and less carefully followed. However, the available evidence cannot indicate the precise ways in which practices differ from those of their European counterparts.

47. If passenger data are revealed to third parties, a range of federal and provincial information and privacy statutes might apply. Federal agencies, including Customs Canada and the RCMP, are regulated by the federal Privacy Act of 1982. Local law-enforcement authorities are regulated under provincial information and privacy statutes, which now exist for the public sector in every Canadian jurisdiction, except Prince Edward Island. Only Quebec’s Bill 68, however, covers records disclosed by airlines to private enterprises under provincial jurisdiction.

48. It is less clear how a data subject could obtain redress against an airline in Canada. No Canadian data protection office, with the exception of Quebec, currently has jurisdiction over the personal information held by the airlines, whether domestic or international. The power of the CAI in Quebec is very tenuous.

49. The airline industry will, however, be one of the first sectors affected by the recent federal effort to extend privacy protection to the private sector in Bill C-54. This bill is based upon the principles within the Canadian Standards Association's Model Code for the Protection of Personal Information, and gives a range of oversight and investigative powers to the Federal Privacy Commissioner.

Sensitive Data in Airline Reservations

(c) *Hong Kong*

The Nature and Circumstances of the Transfer

1. FLYBEST Airlines is a major international carrier which flies into Hong Kong. It has employees in offices and at the airport in Hong Kong, but also contracts with a local company, TAIPAN, to provide check-in services at the airport. This case study takes a hypothetical journey and identifies the multiple transborder transfers of personal information associated with it, before focusing on the protection afforded to the data that is transferred into Hong Kong.

The Booking

2. A citizen of Eurostate, a country in the European Union (EU), flies economy class from Euroville to Hong Kong on a direct FLYBEST flight, then on a code-share JETWELL flight to Sydney.

3. The passenger is a member of FLYBEST's Managers' Club (which automatically includes the 'frequent flyer' programme). He will require a wheelchair at all airports and kosher meals on all flights. FLYBEST knows this from his profile when the flight is booked and his Managers' Club number is provided.

4. The booking of a flight can be made directly from the airline either through a FLYBEST office (in person or by telephone) or through FLYBEST's Internet site. Flights can also be booked through a travel agent who will have indirect access via international reservation systems such as Galileo or Sabre. The origin of the booking does have some subtle implications for how personal data are stored and transmitted (see 'Recommendation 1/98 on Airline Computerised Reservation Systems (CRS)', from the EU's Article 29 Working Party). For this scenario, however, we assume that the booking is made directly through FLYBEST's telephone sales department.

Personal Information Flows - Euroville-to-Hong Kong Flight

5. When the passenger books his flight in Eurostate, a 'Passenger Name Record' (PNR) is created in FLYBEST's Computerised Reservation System (CRS), the database for which is located in Eurostate. PNRs must contain a name, itinerary, phone number, the ticketing option (i.e., by what date it must be paid for), and the name of the person who phoned in the reservation. The fares and taxes payable are calculated automatically (taking account of any special fares) and the amount and method of payment will also be added in due course - if by credit card, the card type, number, expiry date and merchant authorisation code. In this case, the PNR would also hold the request for a special meal and a wheelchair, recorded as internationally recognised codes which have been issued by the International Air Transport Association (IATA). The disability code used indicates that the passenger needs a wheelchair but is not totally immobile. Permanent preferences registered by Managers' Club members are transferred automatically from the Club database into the CRS. Other codes entered on a one-off basis in these fields of the database would indicate such additional characteristics as unaccompanied minor, deportee, prisoner under escort, etc., or special needs for passengers who are not Club members. Seat allocations are generated in advance for First and Business Class passengers, Club members and others with special needs, while seat allocations for most other economy passengers are currently not made until check-in.

6. Some countries, including Hong Kong, now offer electronic visas to speed up passenger processing at ports of entry (and reduce paperwork). Passengers who choose to

take advantage of this system provide FLYBEST with additional information required by the relevant immigration authorities. This is entered into a module within the CRS and transmitted on-line to the immigration authorities concerned - in this case in Canberra, Australia. The visa application is processed and an 'electronic visa' issued to the passenger through FLYBEST's CRS**.**

7. The PNR is held on FLYBEST's mainframe computer in Euroville, to which authorised FLYBEST personnel and agents around the world have access. Between 36 and 48 hours before departure, relevant fields from the PNR are transferred to the Departure Control System (DCS). DCS is a subsidiary database held in Eurostate but, like the CRS, accessible worldwide. The day before the flight, the check-in agents will 'edit' the flight list to make sure there is the appropriate weight distribution, to establish fuel requirements, to order meals, and to ascertain that those with special needs have been properly accommodated.

8. When the passenger checks in for the flight at Euroville Airport, the FLYBEST check-in staff would enter his last name to access his record on the DCS. Check-in staff (whether employees or agents) can also access this information by seat number. At a pre-set time before departure (approximately 30 minutes) a complete list of passengers by seat number is printed and given to the cabin crew; any subsequent last minute changes are notified separately.

9. The records for each flight are purged from the DCS some two hours after the flight has landed. Printed copies of all flight lists are held at Euroville Airport for 12 months.

10. The PNR itself is purged from the CRS between 24 and 48 hours after the completion of the last leg of each journey. It is, however, retained in a separate database for two years for the purpose of management analysis.

11. The FLYBEST flight attendants know from the passenger list about special needs and will probably welcome the passenger by name. He will be given his kosher meals, probably in advance of the general meals service.

12. At Hong Kong airport, the passenger will be met by a TAIPAN employee (or contractor) with a wheelchair and taken to baggage claim, through immigration and customs and to the car-hire check in desk. The car-hire company, and the hotel at which he is staying, have been notified in advance by FLYBEST local staff, responding to an automatically generated request from the CRS. Some hotel and car-hire chains now have an interface to FLYBEST's CRS and would receive the reservation on-line, although this automated transfer would not convey any 'special needs' such as the wheelchair for the passenger.

13. FLYBEST's Managers' Club is sub-contracted - for the East Asia region, to a company called WECARE, located in Singapore, but with an office in Hong Kong. While in Hong Kong, the passenger may contact FLYBEST to confirm his onward flight details and/or seek general assistance. Unlike with some airline clubs, WECARE would not be able to change the bookings for the passenger, although they could make a new flight reservation on the CRS using 'frequent-flyer' points and would refer him to FLYBEST if he wanted to do this.

Personal Information Flows - Hong Kong-to-Sydney Flight

14. On completion of his business in Hong Kong, the passenger takes an onward flight to Sydney. This flight, although it has a FLYBEST number, is in fact a JETWELL service, on a code-share arrangement. At the JETWELL check-in desk, the passenger finds that his relevant details have been automatically transferred from the FLYBEST CRS to the JETWELL system. The details transferred would only be the relevant stage booking, the immediately prior connecting flight (if any) and any special needs, such as the wheelchair

and the kosher meals. 'Second' carriers do not have direct access to FLYBEST's CRS and do not need, or receive, the complete journey details, booking contacts or PNR history.

Overview of the Regulatory Environment for This Case

15. Data users in Hong Kong are subject to the Hong Kong Personal Data (Privacy) Ordinance, and must comply with its six data protection principles. The 1995 Ordinance has put in place a comprehensive regime with an independent supervisory authority - the Privacy Commissioner for Personal Data. The rights conferred under the Ordinance are not confined to residents of Hong Kong. The law protects personal information, including about any identifiable individual - including overseas visitors.

16. Whether FLYBEST, in this scenario, is a data user under the Hong Kong Ordinance will depend on whether it controls the collection, holding, processing or use of personal data in Hong Kong. If all of the data are actually held in Eurostate and only accessed (read) in Hong Kong by personnel of FLYBEST or its agents, then there may not be a data user subject to the Ordinance, but it seems likely that the use of the data by Hong Kong-based personnel (including use for producing the flight lists, and for making any changes) would bring at least some of it under the scope of the Ordinance.

17. Airlines are members of a major trade association, IATA, which has headquarters in Montreal. International airline policy is co-ordinated by the International Civil Aviation Authority (ICAO), a United Nations-affiliated body located in Montreal. FLYBEST and JETWELL are subject to the 1996 ICAO 'Code of Conduct for the Regulation and Operation of Computer Reservation Systems (CRS)'. Article 11 states that 'air carriers, system vendors, subscribers and other parties involved in air transportation are responsible for safeguarding the privacy of personal data included in the CRSs to which they have access, and may not release such data without the consent of the passenger.' The ICAO issues standards and recommended practices for both airlines and members states, but it has no enforcement powers.

Purpose Limitation, Transparency and Opposition

Collection

18. Most of the information recorded by FLYBEST in a PNR is either provided by or on behalf of the passenger, or is generated by FLYBEST (e.g., the flight and seat numbers). The only information obtained from third parties would be the 'approvals' returned by the immigration authorities in destination countries offering electronic visas, authorisations for credit-card debits, and the reference numbers returned from the CRSs of any other carriers involved in the journey.

19. The FLYBEST Airlines 'Conditions of Carriage' declares that:

> 'The Passenger recognises that personal data has been given to Carrier for the purposes of making a reservation for carriage, for obtaining ancillary services, and for facilitating immigration and entry requirements. For these purposes, the Passenger authorises Carrier to retain such data and to transmit it to its own offices, other carriers or the providers of such services, in whatever country they may be located.'

It is not clear how, and in what manner, this assurance is made known to passengers.

20. In Eurostate, and while the PNR is being accessed by FLYBEST personnel in Hong Kong, the collection and use of personal data will be in accordance with policies set by Head Office in Eurostate. Company policy, world-wide, is guided by the requirements

of the Eurostate data protection law. FLYBEST's Hong Kong representative is aware of the Hong Kong Ordinance but operates on the assumption that the company's policies are compliant. For a passenger originating in Eurostate, therefore, limits imposed for the collection of personal data are determined by the requirements of the Eurostate data protection law, as interpreted by company policy and communicated to employees.

Use and disclosure for FLYBESTs purposes

21. The information FLYBEST holds about passengers is used by them, and by other organisations involved in the journey, for the purposes of providing travel and related services. These uses are not only within the reasonable expectation of the passenger but will generally be with at least their implied consent. Depending on whether the Conditions of Carriage cited above are drawn to their attention, this could be taken to be express consent. While FLYBEST itself is subject to Eurostate data protection law, TAIPAN and any Hong Kong-based hotels and car-hire firms which necessarily receive personal information about the passenger are subject to the Hong Kong Personal Data (Privacy) Ordinance. Whether JETWELL is subject to the Hong Kong privacy law depends on an interpretation of a section of the Ordinance which exempts persons 'acting on behalf of others'.

22. Recall also that the passenger is a member of FLYBEST's Managers' Club. There is a separate database of Managers' Club members in each country or region. Most other airlines retain central databases. The East Asia database on FLYBEST’s Managers' Club members in Australia and New Zealand is held in Singapore and managed by WECARE - a United States-based company on contract to FLYBEST. This database holds a profile of the passenger’s flight history, hotel reservation and car-hire needs, frequent-flyer account, and other information (more extensive than the CRS). There is a daily comparison and update of data between the Managers' Club database and FLYBEST's Customer and Marketing database held in Eurostate. WECARE staff have read-only access to FLYBEST's CRS; they are not able to make changes. FLYBEST personnel have limited access to Managers' Club data to provide the 'personalised' service that such customers have come to expect.

23. WECARE may be subject to the Hong Kong privacy law, depending on the interpretation of Section 2(12) on 'agents'. WECARE is at least under strict contractual terms relating to use and disclosure of passenger information, but only FLYBEST, as the client, could take action for breach of those terms. A passenger whose information was misused would not be able to take legal action, except perhaps indirectly against FLYBEST.

Disclosure to third parties for other purposes

24. FLYBEST employees in Hong Kong will have been made aware through induction training, and through a notice on the computer access applications (see below) of the general policy about the disclosure of reservations information. They are reminded that: 'The carriage by air of passengers is a matter of private contract between the airline and the passenger concerned. As a general rule details of that contract should not be given to third parties particularly when the request is made on the telephone.' Employees are told not to disclose information about a passenger, including via the telephone, unless the information is given to:

a) a colleague/another airline or agent for the purpose of reservation booking or ticket issue;
b) the passenger himself and you have taken the necessary steps to ensure that this person is the passenger;
c) some other person and the passenger has clearly consented to this and there is a record of this in the PNR;
d) an appropriate person or organisation in an emergency to prevent injury or damage to someone’s health.

25. Employees are also advised, orally, that requests from the police or law enforcement bodies must be referred to the investigations unit, and those relating to legal proceedings to the legal department. They are also advised that details of medical conditions must not be disclosed without reference to the Senior Medical Officer.

26. FLYBEST's personnel work, however, in a number of different settings that might guide the ways in which these rules are interpreted. In a telephone-sales context, they are quite strictly adhered to. If the person to whom the sales agent is speaking is not travelling, or is not mentioned in the contact field of the booking (such as the name of the secretary), then details cannot be given out.

27. In the airport environment, however, practices may differ. FLYBEST staff and agents will have access to passenger information before, during and after a flight. A greater variety of more urgent requests arise within the airport context, in which such requests might come from the police or other law enforcement authorities, or from Customs and Immigration officials.

28. Requests for personal information from authorities, whether at the airport or to FLYBEST offices, will normally be handled by a supervisor. At the airport, requests from customs or police (usually known personally) are handled informally with no record being kept, unless there is a need for an accompanying 'statement' from an employee. TAIPAN employees at the airport are expected to refer requests to FLYBEST supervisors, although the standard IATA contract for ground handling services does not contain any specific contract terms about confidentiality; however, there are such terms in WECARE's contract. WECARE's policy is to refer all requests from third parties to the client, FLYBEST. Current policy in FLYBEST offices is to ask for identification, and usually a faxed request, but not to enquire any further into the justification, or to try to impose any conditions on use or further disclosure. Request forms are filed but no indication is made on the PNR or Club database. The policies of other carriers such as JETWELL are also not known to FLYBEST, who rely on the passenger's consent for transfer of personal information to other carriers as required (see standard terms above).

29. The major circumstances under which the passenger's records would be accessed after a flight would be if he left a possession by the seat. If the flight attendant or cleaning crew found a possession, FLYBEST or TAIPAN staff would be able to access the PNR by seat number and contact the telephone number on the PNR (up to the time the PNR is deleted, after which the problem would be handled via Eurostate). JETWELL could be expected to have similar arrangements.

30. The deletion of passenger records from the computer system shortly after the completion of a flight should ensure that PNR data will not be available in Hong Kong (and therefore potentially open to misuse or third-party requests) for any length of time. If there are special requests from third parties after the PNR has been archived, they would have to be made in writing and considered in Eurostate under the data protection law.

Data Quality and Proportionality

31. Given the central direction of FLYBEST’s personal-information policy and computer-systems design, any data that are collected in Hong Kong are largely governed, indirectly, by the requirements of the Eurostate data protection law, although it also needs to comply with the Hong Kong Privacy Ordinance. Data are collected in order to fulfil the private contract between the carrier and the passenger concerned. The standard minimum amount of information needed for the creation of a PNR would seem necessary and not excessive to fulfil FLYBEST’s obligations; any further information supplied (about special needs) is presumably provided by or with the consent of the passenger.

32. Some of this information can, however, be very sensitive. Airlines may collect a variety of medical information: physical handicaps, diabetic status, allergic reactions, etc. Some passengers have special dietary needs: kosher meals, no salt, vegetarian, etc., which give clues to religious affiliation or medical conditions. International airlines might also receive other categories of sensitive data, including information on dignitaries, deportees, unaccompanied minors (who might be in the middle of a parent custody dispute), and members of groups who have certain sensitive affiliations, such as some political movements. Some sensitive information is held permanently in the regional Managers' Club databases and this is reconciled daily with FLYBEST's master Customer and Marketing database in Eurostate. Data-quality problems arise from this need for matching, although this will be reduced by the proposed introduction of a new uniform database serving both FLYBEST itself and its Managers' Club contractors. There are no specific provisions in the Hong Kong Ordinance applying higher data protection standards to 'sensitive' classes of data.

33. FLYBEST employees are also advised, orally during induction training to refrain from placing into the central database 'any information or statement about a passenger which may be inaccurate or disparaging or discredit the passenger in any way.' There appears to be no express 'passing on' of this guidance to JETWELL employees acting as FLYBEST's agents, but JETWELL itself can be expected to have a similar policy and training in respect of their own passengers.

Security

34. Security requirements are also directed from Eurostate. None of the PNR data are encrypted. FLYBEST 's CRS, the DCS and the Customer and Marketing database are password-protected for all users - its own staff, check-in agents, and WECARE staff. There are different levels of access depending on status in the organisation. Employees, agents and contractors' staff needing access all have to complete an application form which also serves to remind them about the need for confidentiality. After endorsement by a supervisor as to the level of access required, the applications are processed in Eurostate and authorisation codes (user IDs) are issued. To access the system, users have to input their ID and a self-selected password (which has to be changed at regular intervals). The history of any changes to a PNR is recorded. There is an audit trail of all access to the CRS.

35. WECARE is required by the terms of its contract to maintain a separate operation with dedicated 'front line' staff - i.e., staff cannot service both FLYBEST Managers' Club members and other customers of other clients. WECARE's staff have limited (mainly read only) access to FLYBEST's systems, although WECARE's regional membership data are uploaded and reconciled daily with the FLYBEST Customer and Marketing system. WECARE's separate database of regional Club members is protected in similar ways to the FLYBEST systems.

Access and Rectification

36. Access by passengers to personal information held about them by FLYBEST tends to occur for very practical and mundane reasons (such as checking schedules and preferences), and will normally take place prior to departure. These data can also be accessed formally via the 'subject access' provisions of the Eurostate data protection law, which enables European passengers to check the accuracy, relevance and completeness of information. It is difficult to envisage circumstances under which European passengers would want formally to access or correct their records during the very brief period while they are processed by FLYBEST within Hong Kong. But if they did, the access rights under DPP6 of the Hong Kong Personal Data (Privacy) Ordinance may be available to them.

37. The same access and correction rights under the Hong Kong law are also available if information is lawfully given by FLYBEST to a third party and is controlled from within Hong Kong for other purposes.

Onward Transfer Restrictions

38. Through its CRS, FLYBEST routinely transfers personal information in PNR records between jurisdictions. The Eurostate data protection law has always contained transfer prohibition provisions which could be invoked if there was a perceived risk of a breach of privacy principles as a result of such a transfer. These provisions have been amended to bring them into line with the EU Directive. The issue for this case study is however somewhat different. In assessing adequacy of protection in a third county, the Article 29 Working Party has suggested that one important consideration is the availability of controls on the onward transfer of data to jurisdictions with lesser or no privacy protection.

39. In Hong Kong, organisations holding personal data are subject to express statutory provisions about onward transfer. Section 33 of the Hong Kong Ordinance will prevent data users from transferring personal data outside Hong Kong unless certain conditions are met, with the aim of ensuring that the data will be continue to be protected and handled in accordance with privacy principles. This Section is not yet in force. The Privacy Commissioner has issued further guidance on this provision (Fact Sheet 1, May 1997).

40. When s.33 is brought into force, data users such as FLYBEST will be able to transfer data freely to any places which have been specified by the Privacy Commissioner as having similar laws, without any further steps. It seems likely that EU member states will be declared to have similar laws, and therefore transfers about the passenger back to his home country will not pose any difficulty. But if FLYBEST wants to transfer information about a passenger to a 'third country' which has not been specified, it will only be able to do so if:

- it has reasonable grounds for believing that there is a similar law in force (in the absence of any guidance from the Privacy Commissioner);
- it has obtained the passenger's consent in writing;
- it is in his interests but in circumstances where consent is impracticable to obtain (but likely);
- the use or disclosure involved is an exempt one for the purposes of DPP3; or
- the data user has taken reasonable precautions and exercised ‘all due diligence’ to ensure the data will be handled responsibly.

Fact Sheet 1 suggests that one way of demonstrating 'due diligence' is to use contract terms, and a model contract is included.

41. The inclusion in the Hong Kong law of an 'onward transfer' provision, similar in terms and effect to Articles 25 and 26 of the EU Directive, would appear to satisfy one of the core requirements which EU members are likely to require in order to assess a place as having adequate protection, once s.33 is in force. The breadth of the DPP3 exemptions as applied to s.33 would seem at first sight to weaken the effectiveness of s.33 as a safeguard, but are in fact analogous to the exception provided by Article 26(1)(d) of the Directive.

Remedies

42. FLYBEST has an internal complaints-handling process. Most complaints relate to issues such as pricing, and the flexibility of the tickets purchased, as well as to the flight experience. Complaints about breaches of the privacy principles are rare, and have never been recorded in Hong Kong. Before the flight, complaints are handled through a hierarchy

of service agents, managers and directors. If the complaint occurs after the flight is taken, then it will be referred to the Customer Relations Department.

43. Complaints about privacy breaches by FLYBEST could be made either to the Hong Kong Privacy Commissioner for Personal Data, or to Eurostate Data Protection Registrar. It can sometimes be difficult to work out exactly where responsibility lies and under which legislation it is more appropriately handled. It is expected that the two regulators would co-operate in assessing an alleged breach and advising the complainant accordingly.

44. Whichever supervisory authority handled the complaint, there are enforceable remedies available to the complainant under both laws, including the possibility of compensation, and an independent appeal process

Accountability

45. Theoretically, FLYBEST's employees, agents and sub-contractors in Hong Kong should be given exactly the same guidance about personal-information practices as their counterparts in Eurostate. Written policies, already cited, are available online and drawn to staff's attention during induction. There is no privacy officer, designated as such, in FLYBEST's regional organisational structure, but security personnel assume broad responsibility for monitoring access to the central reservation system.

46. Data users in Hong Kong are held accountable for compliance with the Ordinance through the Privacy Commissioner for Personal Data, who has a range of powers, including the power to conduct inspections.

Conclusions

47. For airlines like FLYBEST, guided by an established set of data protection standards within their 'home country' legislation, there should be little difference between practices in Hong Kong (or in any other third country) and those in the home country, in this case, Eurostate. In the case of Hong Kong, compliance should be reinforced by the general requirement to comply with the similar rules in the Hong Kong Privacy Ordinance for data controlled within Hong Kong. Only systematic on-site auditing can, of course, determine whether or not company policy and guidance is followed.

48. For other foreign carriers such as JETWELL, operating out of Hong Kong and involved in carriage of a FLYBEST passenger, it is probable that the rules are less stringent and less carefully followed. For example, Australian businesses such as JETWELL do not have to comply with general data protection principles in their home country. However, the available evidence cannot indicate the precise ways in which practices differ from those of their European counterparts. Yet, to the extent that FLYBEST's Hong Kong activities are subject to the Hong Kong law, then so too would be JETWELL's activities; i.e., if they control data in Hong Kong, then they are subject to the Ordinance.

49. The Hong Kong Privacy Commissioner has jurisdiction over most data users who 'control' personal data in Hong Kong, including users based overseas, and whether their control is exercised directly or through local employees or agents. The practicalities of exercising the Commissioner's formal powers against an overseas-based data user have yet to be tested. At the least, however, he could receive complaints and liaise informally with the Eurostate Data Protection Authority to establish who had jurisdiction and could best investigate an alleged breach of privacy by FLYBEST or its agents in Hong Kong.

50. If passenger data are revealed to third parties in Hong Kong, then the Hong Kong Privacy Ordinance would apply to their handling of those data.

51. Overall, for transfers of personal data into Hong Kong associated with airline travel, the Ordinance appears to contain both privacy principles and accountability mechanisms equivalent to those set out in the EU Directive. The law applies comprehensively to all organisations in both the private and the public sector, and the rights granted by the Ordinance apply to all individuals including foreign visitors. Therefore, to the extent that personal data involved in an airline passenger's journey through Hong Kong are controlled by a data user in Hong Kong, they will be protected by the Ordinance.

52. If FLYBEST is subject to the Hong Kong Ordinance, its apparent failure to draw passengers' attention to the personal-information section of the 'Conditions of Carriage' could constitute a breach of the transparency requirements of the Ordinance.

53. With this qualification, and once the onward transfer provisions of s.33 are in force, the privacy protection regime in Hong Kong as it applies to the handling of airline data would appear to meet all the main requirements that have been suggested as necessary to be assessed as 'adequate' for the purposes of Article 25.

Sensitive Data in Airline Reservations

(d) *Japan*

The Nature and Circumstances of the Transfer

1. TRANSPACIFIC Airlines (TPA) is a major international carrier, which operates direct non-stop flights from the European Union (EU) to Tokyo.

The Booking

2. A citizen of a Eurostate, a country in the EU, flies economy class from Euroville to Tokyo's Narita airport via TPA.

3. The passenger is a member of TPA's Managers' Club (which automatically includes the 'frequent flyer' programme). He will require a wheelchair at all airports and kosher meals on all flights. TPA knows this from his profile when the flight is booked and his Managers' Club number is provided.

4. The booking of a flight directly from the airline is one of four ways that international bookings might take place. Thus our passenger could also reserve the flight through a travel agent who will have access to international reservation systems such as Galileo or Sabre. He might reserve through TPA's Internet site. He might call the toll-free number associated with TPA's frequent flyer programme. The origin of the booking does have some subtle implications for how personal data are stored and transmitted (see 'Recommendation 1/98 on Airline Computerised Reservation Systems', from the EU's Article 29 Working Party). For this scenario, however, we assume that the booking is made directly through TPA's telephone sales department.

Personal Information Flows - Euroville-to-Tokyo Flight

5. When the passenger books his flight in Eurostate, a 'Passenger Name Record' (PNR) is created in TPA's Computerised Reservation System (CRS), the database for which is located in Eurostate. PNRs must contain a name, itinerary, phone number, the ticketing option (i.e., by what date it must be paid for), and the name of the person who phoned in the reservation. The fares and taxes payable are calculated automatically (taking account of any special fares) and the amount and method of payment will also be added in due course - if by credit card, the card type, number, expiry date and merchant authorisation code. In this passenger's case, the PNR would also hold the request for a special meal and a wheelchair, accessible by internationally recognised codes which have been issued by the International Air Traffic Authority (IATA). Permanent preferences registered by the Managers' Club are transferred automatically from the Club database into the CRS. Other codes entered on a one-off basis in these fields of the database would indicate such additional characteristics as unaccompanied minor, deportee, prisoner under escort, etc., or special needs for passengers who are not Club members. Seat allocations are generated in advance for First and Business Class passengers, Club members and others with special needs, while seat allocations for most other economy passengers are currently not made until check-in.

6. The PNR is held on TPA's mainframe computer in Euroville, to which authorised TPA personnel around the world have access. Between 36 and 48 hours before departure, relevant fields from the PNR are transferred to the Departure Control System (DCS). DCS is a subsidiary database held in Eurostate but, like the CRS, accessible worldwide. The day before the flight, the check-in agents will 'edit' the flight list to make sure there is the appropriate weight distribution, to establish fuel requirements, to order meals, and to ascertain that those with special needs have been properly accommodated.

7. When the passenger checks in for the flight at Euroville Airport, the TPA check-in staff would enter his last name to access his record on the DCS. Check-in staff (whether employees or agents) can also access this information by seat number. At a pre-set time before departure (approximately 30 minutes) a complete list of passengers by seat number is printed and given to the cabin crew; any subsequent last minute changes are notified separately.

8. The records for each flight are purged from the DCS some two hours after the flight has landed. Printed copies of all flight lists are held at Euroville Airport for 12 months.

9. The PNR itself is purged from the CRS between 24 and 48 hours after the completion of the last leg of each journey. It is, however, retained in a separate database for two years for the purpose of management analysis.

10. The TPA flight attendants know from the passenger list about special needs and will probably welcome the passenger by name. He will be given his kosher meals, probably in advance of the general meals service.

11. On the flight, he is asked to fill in an embarkation card from Japanese immigration. He is required to provide the following information: name, date and place of birth, nationality, passport number, flight number, address in Japan, occupation, and gender. On arrival, the passenger will be met by TPA's special services and will be taken to baggage claim and through immigration and customs. Here he will surrender his embarkation card. Narita Airport uses extensive video-surveillance technology. It is certain that the passenger's image will be captured on videotape sometime during this initial arrival period.

12. Having cleared Customs and Immigration, the passenger leaves the airport by a hired car and proceeds to a downtown hotel. The car-hire company and the hotel can receive reservations directly through TPA's CRS, although the transfer of data would not convey special-needs information such as the use of a wheelchair.

Overview of the Regulatory Environment for this Case

13. Japan has no legislated data protection standards that apply to data processed in airline reservation systems. Moreover the new supervisory authority established by the Ministry of Trade and Industry will not have jurisdiction over airlines. It is anticipated that the Privacy Protection Mark system will apply to personal data of this nature. To the extent that passenger information might find its way to governmental agencies, the 1988 Act for the Protection of Computer Processed Personal Data might offer some protection.

14. No sectoral code of practice applying to airline information could be cited by Japanese officials, although there have been some preliminary discussions within the Ministry of Transportation. Nor has Japan declared its adherence to the 1996 'Code of Conduct for the Regulation and Operation of Computer Reservation Systems (CRS), from the International Civil Aviation Organisation. At the moment, one can assume, therefore, that no data protection rules are embedded in Japanese air transport regulations.

15. Current Japanese data protection policy is based on distinction between 'highly confidential data' circulated internationally, and other forms of data. In some sectors (e.g., personal-credit data), statutory protections will be introduced. No Japanese documents, however, appear to recognise that highly sensitive data might be transmitted through airlines and their reservation systems.

Purpose Limitation, Transparency and Opposition

Collection

16. The TPA Airlines 'Conditions of Carriage' declares that:

> 'The Passenger recognises that personal data has been given to Carrier for the purposes of making a reservation for carriage, for obtaining ancillary services, and for facilitating immigration and entry requirements. For these purposes, the Passenger authorises Carrier to retain such data and to transmit it to its own offices, other carriers or the providers of such services, in whatever country they may be located.'

It is not clear how, and in what manner, this assurance is made known to passengers.

17. In Eurostate, and while the PNR is being accessed by TPA personnel in Japan, the collection and use of personal data will be in accordance with policies set by Head Office in Eurostate. Company policy, world-wide, is guided by the requirements of the Eurostate data protection law. For a passenger originating in Eurostate, therefore, limits imposed for the collection of personal data are determined by the requirements of the Eurostate data protection law, as interpreted by company policy and communicated to employees.

Use and disclosure for TPA's purposes

18. The information TPA holds about passengers is used by them, and by other organisations involved in the journey, for the purposes of providing travel and related services. These uses are not only within the reasonable expectation of the passenger but will generally be with at least their implied consent. Depending on whether the Conditions of Carriage cited above are drawn to their attention, this could be taken to be express consent. Information on the need for a wheelchair will be recorded on the PNR and collected on the flight. It is passed on to Narita airport officials via the CRS. Flight editors and arrival service staff can access this information for up to six months after the termination of the flight.

19. The passenger is a member of TPA's Managers' Club. This database holds a more complete profile of the passenger's flight history, hotel reservation and car-hire needs, frequent-flyer history, and other information. TPA personnel have complete access to these data to provide the 'personalised' service that such customers have come to expect. It should be noted, however, that TPA retains a separate database of its frequent-flyer passengers (including those receiving special services) in each country or region, including Japan. Nobody at Narita airport, however, has access to this database or to frequent-flyer history.

Disclosure to third parties for other purposes

20. TPA employees in Japan will have been made aware of the general policy about the disclosure of reservations information and are advised not to give out information regarding TPA passengers. Employees are also advised that requests from police or law-enforcement bodies should only be responded to after an official letter of request. TPA personnel work, however, in a number of different settings that might guide the ways in which these rules are interpreted. No other evidence is available of further controls on release of PNR data.

21. The major circumstances under which the passenger's records would be accessed after a flight would be if he left a possession by the seat. If the flight attendant or cleaning crew found a possession, TPA staff would be able to access the PNR by seat number and contact the telephone number on the PNR. This would only be possible up to the time the PNR is deleted, after which the problem is handled via Eurostate.

22. The deletion of passenger records from the computer system shortly after the completion of a flight should ensure that PNR data will not be available in Japan (and therefore potentially open to misuse or third-party requests) for any length of time. If there are special requests from third parties after the PNR has been archived, they would have to be made in writing and considered in Eurostate under the data protection law.

Data Quality and Proportionality

23. Given the central direction of TPA's personal-information policy and computer-system design, limitations on data types that are collected are largely governed by the requirements of the Eurostate data protection law. Data are collected in order to fulfil the private contract between the carrier and the passenger concerned. The standard minimum amount of information needed for the creation of a PNR would seem necessary and not excessive to fulfil TPA's obligations; any further information supplied (about special needs) is presumably provided by or with the consent of the passenger.

24. Some of this information can, however, be very sensitive. Airlines may collect a variety of medical information: physical handicaps, diabetic status, allergic reactions, etc. Some passengers have special dietary needs: kosher meals, no salt, vegetarian, etc., which give clues to religious affiliation or medical conditions. International airlines might receive other categories of sensitive data, including information on dignitaries, deportees, unaccompanied minors (who might be in the middle of a parental-custody dispute), and members of groups who have certain sensitive affiliations, such as some political movements.

25. Flight lists (both incoming and return) will be held for six months at Narita airport, before being deleted. This retention period is longer than in other destination jurisdictions.

Security

26. Security requirements are also directed from Eurostate. None of the PNR data is encrypted. TPA's CRS, the DCS and the Customer and Marketing database are password-protected for all users - its own staff and check-in agents. There are different levels of access depending on status in the organisation. Employees, agents and contractors' staff needing access all have to complete an application form which also serves to remind them about the need for confidentiality. After endorsement by a supervisor as to the level of access required, the applications are processed in Eurostate and authorisation codes (user IDs) are issued. To access the system, users have to input their ID and a self-selected password (which has to be changed at regular intervals). The history of any changes to a PNR is recorded. There is an audit trail of all access to the CRS. However, it has not been possible to verify the extent to which any of these security procedures are complied with in Japan.

Access and Rectification

27. Access by passengers to personal information held about them by TPA tends to occur for practical and mundane reasons (such as checking schedules and preferences), and will normally take place prior to departure. These data can also be formally accessed via the 'subject access' provisions of the Eurostate data protection law, which enables European passengers to check the accuracy, relevance and completeness of information. If a European passenger would want to access their records during the six-month period that they are held at Narita Airport, there would be no statutory reason why TPA would have to comply with such a request.

28. If the data were provided to a Japanese government agency, the 1988 Act for the Protection of Computer Processed Personal Data might be invoked, which provides for rights of access and correction.

Onward Transfer Restrictions

28. TPA does not transfer personal information from PNR records to officials within other jurisdictions. If, for example, law-enforcement authorities from another country were interested in a passenger list, they would have to apply in writing to TPA's Eurostate officials.

Remedies

29. TPA has an internal complaints-handling process. Most complaints relate to issues such as pricing and the flexibility of the tickets purchased, and tend to arise before the flight is taken. Complaints about breaches of the privacy principles are rare. Before the flight, complaints are handled through a hierarchy of service agents, managers and directors. If the complaint occurs after the flight is taken, it will be referred to the Customer Relations Department.

30. No governmental agency would provide remedies under Japanese law if personal data were improperly processed by TPA. Remedies through the courts would be exceedingly difficult.

Accountability

31. Theoretically, TPA’s employees, agents and sub-contractors in Japan should be given exactly the same guidance about personal information practices as their counterparts in Eurostate. Written policies, already cited, are disseminated in paper format and online. There is no privacy officer, designated as such, but security personnel assume broad responsibility for monitoring access to the central reservation system.

Conclusions

32. For airlines like TPA, guided by a more established set of data protection standards within their 'home country' legislation, there should be little difference between practices in Japan (or in any other third country) and those in the home country, in this case, Eurostate. Only systematic on-site auditing can, of course, determine whether or not guidance is followed; none could be cited.

33. It is not clear how a data subject could obtain redress against an airline in Japan. No Japanese supervisory authority has jurisdiction over the personal information held by the airlines, whether domestic or international. Relief through the courts would be prohibitively costly.

34. In summary, a good level of compliance can only, at best, be inferred because of central policy direction from Eurostate, but it is not easy to determine whether central policy is actual followed in practice in the Japanese environment. In terms of help for data subjects and remedies, however, it is difficult to see how a transfer of this type of personal data approaches the standards for adequate protection.

Sensitive Data in Airline Reservations

(e) *New Zealand*

The Nature and Circumstances of the Transfer

1. FLYBEST Airlines is a major international carrier. It has no direct flights into New Zealand, but has a code-share arrangement with an Australian airline, JETWELL, for flights between New Zealand and the USA. FLYBEST has employees in offices in New Zealand, but not at airports. This case study takes a hypothetical journey and identifies the multiple transborder transfers of personal information associated with it, before focusing on the protection afforded to the data that is transferred into New Zealand.

The Booking

2. A citizen of Eurostate, a country in the European Union (EU), has flown FLYBEST from Euroville to Australia, and through them has booked a connecting economy class flight from Sydney to Auckland, New Zealand on the New Zealand airline SOUTHFLIGHT. He is then booked to fly from Auckland to Los Angeles on a FLYBEST/JETWELL code-share flight, before picking up a FLYBEST flight back to Euroville.

3. The passenger is a member of FLYBEST's Managers' Club (which automatically includes the 'frequent flyer' programme). He will require a wheelchair at all airports and kosher meals on all flights. FLYBEST knows this from his profile when the flight is booked and his Managers' Club number is provided.

4. The booking of a flight can be made directly from the airline either through a FLYBEST office (in person or by telephone) or through FLYBEST's Internet site. Flights can also be booked through a travel agent who will have indirect access via international reservation systems such as Galileo or Sabre. The origin of the booking does have some subtle implications for how personal data are stored and transmitted (see 'Recommendation 1/98 on Airline Computerised Reservation Systems', from the EU's Article 29 Working Party). For this scenario, however, we assume that the booking is made directly through FLYBEST's telephone sales department.

Personal Information Flows - Euroville-to-Auckland Flight

5. When the passenger books his flight in Eurostate, a 'Passenger Name Record' (PNR) is created in FLYBEST's Computerised Reservation System (CRS), the database for which is located in Eurostate. PNRs must contain a name, itinerary, phone number, the ticketing option (i.e., by what date it must be paid for), and the name of the person who phoned in the reservation. The fares and taxes payable are calculated automatically (taking account of any special fares) and the amount and method of payment will also be added in due course - if by credit card, the card type, number, expiry date and merchant authorisation code. The PNR will also show the stages of the journey on other airlines, with a reference number returned automatically through an interface with their CRSs. In this passenger's case, the PNR would also hold the request for a special meal and a wheelchair, recorded as internationally recognised codes which have been issued by the International Air Transport Association (IATA). The disability code used indicates that the passenger needs a wheelchair but is not totally immobile. Permanent preferences registered by Managers' Club members are transferred automatically from the Club database into the CRS. Other codes entered on a one-off basis in these fields of the database would indicate such additional characteristics as unaccompanied minor, deportee, prisoner under escort, etc., or special needs for passengers who are not Club members. Seat allocations are generated in advance for First and Business Class passengers, Club members and others

with special needs, while seat allocations for most other economy passengers are currently not made until check-in.

6. The PNR is held on FLYBEST's mainframe computer in Euroville, to which authorised FLYBEST personnel and agents around the world have access. Between 36 and 48 hours before departure, relevant fields from the PNR are transferred to the Departure Control System (DCS). DCS is a subsidiary database held in Eurostate but, like the CRS, accessible worldwide. The day before the flight, the check-in agents will 'edit' the flight list to make sure there is the appropriate weight distribution, to establish fuel requirements, to order meals, and to ascertain that those with special needs have been properly accommodated.

7. When the passenger checks in for the flight at Sydney, the SOUTHFLIGHT check-in staff would find his relevant details on their own reservation/departure control system, to which an entry would have been automatically transferred by FLYBEST's CRS. The details transferred would only be the relevant stage booking, the immediately prior connecting flight (if any) and any special needs. 'Second' carriers do not have direct access to FLYBEST's CRS and do not need, or receive, the complete journey details, booking contacts or PNR history.

8. Assuming SOUTHFLIGHT's system is similar to FLYBEST's, it would generate a printed passenger list for the cabin crew. The precise rules about access, retention periods etc. that apply within SOUTHFLIGHT's system are not known to FLYBEST.

9. The PNR itself is purged from FLYBEST's on-line system between 24 and 48 hours after the completion of the last leg of each journey. It is, however, retained in a separate database for two years for the purpose of management analysis.

10. At Auckland airport, the passenger is taken in a wheelchair by a SOUTHFLIGHT employee or agent to baggage claim, through immigration and customs and to the car-hire check-in desk. The car-hire company, and the hotel at which he is staying, have been notified in advance by FLYBEST local staff (in Australia), responding to an automatically generated request from the CRS. Some hotel and car-hire chains now have an interface to FLYBEST's CRS and would receive the reservation on-line, although this automated transfer would not convey any 'special needs' such as the wheelchair.

11. FLYBEST's Managers' Club is sub-contracted - in New Zealand and Australia to a company called GOODCARE, located in Melbourne, Australia. While in New Zealand, the passenger may contact FLYBEST to confirm his onward flight details and/or seek general assistance. Unlike with some airline clubs, GOODCARE would not be able to change the bookings for the passenger, although they could make a new flight reservation on the CRS using 'frequent-flyer' points, and would refer the passenger to FLYBEST if he wanted to do this.

Personal Information Flows - Auckland-to-Los Angeles Flight

12. On completion of his business in New Zealand, the passenger takes an onward flight to Los Angeles with JETWELL, which is a code-share service with FLYBEST. On check-in at Auckland, he finds again that his relevant details, including special needs, have been transferred to JETWELL's computer system. The wheelchair and kosher meals are ready when required.

Overview of the Regulatory Environment in This Case

13. FLYBEST and JETWELL, while operating in New Zealand, and SOUTHFLIGHT (as a New Zealand business), are subject to the New Zealand Privacy Act 1993, although if JETWELL or SOUTHFLIGHT hold data purely as agent for FLYBEST, they are not data

users for that data (section 3(4)). The Act includes both privacy standards (eleven principles) and enforcement and complaint mechanisms. After a transitional period, the Act has been fully in force since 1996. The New Zealand Privacy Commissioner has issued a considerable amount of guidance material for businesses on compliance with the Act, and a wide range of training has been offered. The New Zealand Privacy Act makes provision for sector or activity codes of practice which can substitute for the 'default' principles, but there have been no such codes issued to date that affect FLYBEST's activities.

14. Airlines are members of a major trade association, IATA, which has headquarters in Montreal. International airline policy is co-ordinated by the International Civil Aviation Authority (ICAO), a United Nations-affiliated body located in Montreal. FLYBEST, JETWELL and SOUTHFLIGHT are subject to the 1996 ICAO 'Code of Conduct for the Regulation and Operation of Computer Reservation Systems (CRS)'. Article 11 states that 'air carriers, system vendors, subscribers and other parties involved in air transportation are responsible for safeguarding the privacy of personal data included in the CRSs to which they have access, and may not release such data without the consent of the passenger.' The ICAO issues standards and recommended practices for both airlines and members states, but it has no enforcement powers.

Purpose Limitation, Transparency and Opposition

Collection

15. Most of the information recorded by FLYBEST in a PNR is either provided by or on behalf of the passenger or is generated by FLYBEST (e.g., the flight and seat numbers). The only information obtained from third parties would be the 'approvals' returned by the immigration authorities in destination countries offering electronic visas, authorisations for credit-card debits, and the reference numbers returned from the CRSs of any other carriers involved in the journey.

16. The FLYBEST Airlines 'Conditions of Carriage' declares that:

> 'The Passenger recognises that personal data has been given to Carrier for the purposes of making a reservation for carriage, for obtaining ancillary services, and for facilitating immigration and entry requirements. For these purposes, the Passenger authorises Carrier to retain such data and to transmit it to its own offices, other carriers or the providers of such services, in whatever country they may be located.'

It is not clear how, and in what manner, this assurance is made known to passengers.

17 In Eurostate, and while the PNR is being accessed by FLYBEST personnel in New Zealand, the collection and use of personal data will be in accordance with policies set by Head Office in Eurostate. Company policy, worldwide, is guided by the requirements of the Eurostate data protection law. For a FLYBEST passenger originating in Eurostate, therefore, limits on the collection of personal data are determined principally by the requirements of the Eurostate data protection law, as interpreted by company policy and communicated to employees.

Use and disclosure for FLYBEST's purposes

18. The information FLYBEST holds about passengers is used by them, and by other organisations involved in the journey, for the purposes of providing travel and related services. These uses are not only within the reasonable expectation of the passenger but will generally be with at least their implied consent. Depending on whether the Conditions of Carriage cited above are drawn to their attention, this could be taken to be express consent. While FLYBEST itself is subject to the Eurostate data protection law, SOUTHFLIGHT and any New Zealand-based hotels and car-hire firms which necessarily

receive personal information about passengers are subject to the New Zealand Privacy Act. JETWELL may also be subject to this Act.

19. FLYBEST personnel in New Zealand will have limited access to Managers' Club data, held by GOODCARE in Melbourne Australia, to provide 'personalised' service. GOODCARE holds no data in New Zealand and is not therefore subject to the New Zealand Privacy Act. GOODCARE is at least under strict contractual terms relating to use and disclosure of passenger information, but only FLYBEST, as the client, could take action for breach of those terms. A passenger whose information was misused by GOODCARE would not be able to take legal action, except perhaps indirectly against FLYBEST.

Disclosure to third parties for other purposes

20. FLYBEST employees in New Zealand will have been made aware through induction training, and through a notice on the computer access applications (see below), of the general policy about the disclosure of reservations information. They are reminded that: 'The carriage by air of passengers is a matter of private contract between the airline and the passenger concerned. As a general rule details of that contract should not be given to third parties particularly when the request is made on the telephone.' Employees are told not to disclose information about a passenger, including via the telephone, unless the information s given to:

- a colleague/another airline or agent for the purpose of reservation booking or ticket issue;
- the passenger himself and you have taken the necessary steps to ensure that this person is the passenger;
- some other person and the passenger has clearly consented to this and there is a record of this in the PNR;
- an appropriate person or organisation in an emergency to prevent injury or damage to someone’s health.

21. Employees are also advised orally that requests from the police or law-enforcement bodies must be referred to the investigations unit, and those relating to legal proceedings to the legal department. They are also advised that details of medical conditions must not be disclosed without reference to the Senior Medical Officer.

22. FLYBEST personnel work, however, in a number of different settings that might guide the ways in which these rules are interpreted. In a telephone-sales context, they are quite strictly adhered to. If the person to whom the sales agent is speaking is not travelling, or is not mentioned in the contact field of the booking (such as the name of a secretary), then details cannot be given out.

23. In the airport environment, however, practices may differ. SOUTHFLIGHT and JETWELL personnel will have access to information about the passenger before, during and after his flight - in SOUTHFLIGHT's case, whatever has been transferred to their system - while some JETWELL staff, as agents for FLYBEST, have direct access to FLYBEST's CRS, where passengers' data will be held for 24 to 48 hours after completion of the flight. A greater variety of more urgent requests arise within the airport context. In a New Zealand airport, such requests might come from the police or from customs and immigration officials.

24. Requests for personal information from authorities, whether at the airport or to FLYBEST offices, are normally handled by a supervisor. Current policy in FLYBEST offices is to ask for identification, and usually a faxed request, but not to enquire any further into the justification, or to try to impose any conditions on use or further disclosure. Request forms are filed but no indication is made on the PNR or Club database. The exact practice followed by agents or contractors including JETWELL employees at the airports and by GOODCARE is not known by FLYBEST. While there is an expectation that they will have similar safeguards, there are no specific terms about confidentiality in the standard

IATA contract for ground handling services, although there are such terms in GOODCARE's contract. The policies of SOUTHFLIGHT are also not known to FLYBEST, who rely on the passenger's consent for transfer of personal information to other carriers as required (see standard terms above). However, SOUTHFLIGHT, as a New Zealand business, is bound by the New Zealand Privacy Act 1993, which includes both privacy standards and enforcement and complaint mechanisms.

25. Any New Zealand recipient of personal information about passengers, whether from FLYBEST, JETWELL, SOUTHFLIGHT or GOODCARE, would also be bound by the New Zealand Privacy Act, which applies to both public and private sector agencies. Section 10 of the Act expressly extends the application of the security, accuracy, retention and use and disclosure limitation principles to information held by an agency that it has transferred out of New Zealand.

26. The major circumstances under which a passenger's records would be accessed after a flight would be if he left a possession by the seat. If the flight attendant or cleaning crew found a possession, JETWELL or FLYBEST would be able to access the CRS or DCS by seat number and contact the telephone number on the PNR (up to the time the PNR is deleted, after which it would have to be handled via Eurostate). SOUTHFLIGHT could be expected to have a similar facility.

27. The deletion of passenger records from the computer system shortly after the completion of a flight should ensure that PNR data will not be available outside the company for any length of time. Third-party requests for access after the PNR has been archived would have to be made in writing and considered in Eurostate under the data protection law.

Data Quality and Proportionality

28. Given the central direction of FLYBEST's personal information policy and computer systems design, the data that are collected in New Zealand are largely governed, indirectly, by the requirements of the Eurostate Data Protection Act. Data are collected in order to fulfil the private contract between the carrier and the passenger concerned. The standard minimum amount of information needed for the creation of a PNR would seem necessary and not excessive to fulfil FLYBEST's obligations; any further information supplied (about special needs) is presumably provided by or with the consent of the passenger.

29. Some of this information can, however, be very sensitive. Airlines may collect a variety of medical information: physical handicaps, diabetic status, allergic reactions, etc. and so on. Some passengers will have special dietary needs: kosher meals, no salt, vegetarian, etc. which give clues to religious affiliation or medical conditions. International airlines might also receive other categories of sensitive data, including information on dignitaries, deportees, unaccompanied minors (who might be in the middle of a parental-custody dispute), and members of groups who have certain sensitive affiliations, such as some political movements. Some sensitive information is held permanently in the regional Managers' Club databases and this is reconciled daily with FLYBEST's master Customer and Marketing database in Eurostate. Data-quality problems arise from this need for matching, although this will be reduced by the proposed introduction of a new uniform database serving both FLYBEST itself and its Managers' Club contractors.

30. No sensitive data are processed about passengers without their knowledge and consent, but this is in any case an issue under the 'home country' data protection law. The fact that the New Zealand Privacy Act does not provide any special protection for sensitive data does not change the level of protection the data enjoy once transferred to New Zealand.

31. FLYBEST employees are also advised, orally in induction training, to refrain from placing into the central database 'any information or statement about a passenger which may be inaccurate or disparaging or discredit the passenger in any way.' There appears to be no express 'passing on' of this guidance to SOUTHFLIGHT employees acting as FLYBEST's agents, but SOUTHFLIGHT itself can be expected to have a similar policy and training in respect of their own passengers.

Security

32. Security requirements are also directed from Eurostate. None of the PNR data is encrypted. FLYBEST's CRS, the DCS and the Customer and Marketing database are password-protected for all users - their own staff, check-in agents, and GOODCARE staff. There are different levels of access depending on status in the organisation. Employees, agents and contractors' staff needing access all have to complete an application form which also serves to remind them about the need for confidentiality. After endorsement by a supervisor as to the level of access required, the applications are processed in Eurostate and authorisation codes (user IDs) are issued. To access the system, users have to input their ID and a self-selected password (which has to be changed at regular intervals). The history of any changes to a PNR is recorded. There is an audit trail of all access to the CRS.

33. GOODCARE is required by the terms of its contract to maintain a separate operation with dedicated 'front line' staff - i.e., staff cannot service both FLYBEST Management Club members and other customers of other clients. GOODCARE's staff have limited (mainly read-only) access to FLYBEST's systems, although GOODCARE's regional membership data are uploaded and reconciled daily with the FLYBEST Customer and Marketing system. GOODCARE's separate database of regional Club members is protected in similar ways to the FLYBEST systems.

Access and Rectification

34. Access by passengers to personal information held about them by FLYBEST tends to occur for very practical and mundane reasons (such as checking schedules and preferences), and will normally take place prior to departure. These data can also be accessed formally via the 'subject access' provisions of the Eurostate data protection law, or, while a non-resident is in New Zealand, under IPP6 of the New Zealand Act**.** However, it is difficult to envisage circumstances under which European passengers would want formally to access or correct their records during the very brief period while they are processed by FLYBEST within New Zealand.

35. If, however, information is lawfully given by FLYBEST to a third party and is retained within New Zealand for other purposes, the access and correction rights enjoyed by citizens and permanent residents are not available to a non-resident once he or she has left the country (s.34 of the Privacy Act).

Onward Transfer Restrictions

36. Through its CRS, FLYBEST routinely transfers personal information in PNR records between jurisdictions. The Eurostate data protection law does contain transfer prohibition provisions which can be invoked if there is a perceived risk of a breach of privacy principles as a result of such a transfer. These provisions are currently being amended to bring them into line with the Directive. The issue for this case study is however somewhat different. In assessing adequacy of protection in a third county, the Article 29 Working Party has suggested that one important consideration is the availability of controls on the onward transfer of data to jurisdictions with lesser or no privacy protection. In New Zealand, while there is no express statutory provision about onward transfer, all

organisations holding personal data are subject to the Privacy Act's security principle (IPP5), which says:

> 'that if it is necessary for the record to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of information.' (Information Principle 5 (b), Section 6, Privacy Act 1993.)

37. This could arguably be invoked to prevent an organisation knowingly transferring data outside New Zealand without taking steps to protect the data, such as imposing appropriate terms and conditions in any contract. However, this provision could not be used to ensure compliance by the recipient with any of the other principles, and only applies to the provision of services, not to the release of information for a third party's own purposes.

Remedies

38. FLYBEST has an internal complaints-handling process. Most complaints relate to issues such as pricing and the flexibility of the tickets purchased, as well as to the flight experience. Complaints to FLYBEST about breaches of the privacy principles are rare, and have never been recorded in New Zealand. Before the flight, complaints are handled through a hierarchy of service agents, managers and directors. If the complaint occurs after the flight is taken, then it will be referred to the most appropriate branch of the Customer Relations Department**.**

39. Under the New Zealand Privacy Act, individuals can complain to the Privacy Commissioner about alleged breaches of any of the privacy principles, or of the procedures relating to requests for access or correction. This right applies in most cases to any individual about whom data is held - they do not have to be New Zealand citizens or even residents, with the exception that the access and correction rights (IPPs 6 and 7) do not apply to non-residents unless they are actually in New Zealand. With this exception, a foreign national would enjoy all the rights given to individuals under the law.

40. If all of the data handling in New Zealand associated with FLYBEST's operations were carried out by an agent (such as JETWELL or SOUTHFLIGHT) which had no independent control of the data, and FLYBEST had no presence in the country, then by virtue of s.3(4) of the Privacy Act, it might be difficult to hold anyone accountable. But because control of the passenger data is in effect shared, and because FLYBEST (and JETWELL) do have employees in New Zealand, there should be no jurisdictional gap.

41. The Commissioner's staff could assist an overseas passenger of an airline holding data in New Zealand and try to conciliate or mediate his complaint. If this is unsuccessful, the Commissioner can refer the matter to a separate Proceedings Commissioner, who will in turn decide whether to take the case to the Complaints Review Tribunal. The Tribunal can make an order prohibiting a repetition of the action complained about, and/or require the interference with privacy to be put right. The Tribunal can also require the respondent agency to pay damages or compensation.

42. It should be noted that very few complaints proceed as far as the Tribunal - most are resolved at an earlier stage. Also, there is a substantial complaints handling backlog due to resource constraints, with individuals typically having to wait twelve months for investigation of their matter to even begin, unless it is assessed as urgent.

43. An overseas passenger would also be able to complain about the acts and practices of FLYBEST to the Eurostate Data Protection Commissioner. In any cases where jurisdiction was unclear, the New Zealand Commissioner and the Eurostate Commissioner

could co-operate to ensure that the complainant is not disadvantaged, and is able to use the optimum channels for obtaining a remedy.

Accountability

44. Theoretically, FLYBEST's employees, agents and sub-contractors in New Zealand should be given exactly the same guidance about personal information practices as their counterparts in Eurostate. Written policies, already cited, are available online and drawn to staff's attention during induction. There is no privacy officer, designated as such, in FLYBEST's regional organisational structure, but security personnel assume broad responsibility for monitoring access to the central reservation system.

45. The issue of who was responsible for any specific action in relation to FLYBEST passenger data - i.e., FLYBEST, JETWELL or SOUTHFLIGHT - would be decided in law on a case by case basis, but contractual arrangements could help to clarify this.

Conclusions

46. For airlines like FLYBEST, guided by established set of data protection standards within their 'home country' legislation, there should be little difference between practices in New Zealand (or in any other third country) and those in the home country - in this case, Eurostate. Only systematic on-site auditing can, of course, determine whether or not company policy and guidance (or legal requirements) are being followed.

47. For the carriers involved in this case, similar rules to those in the Eurostate law apply under the New Zealand Privacy Act, provided they are not merely agents. In this scenario, employees of FLYBEST, JETWELL and SOUTHFLIGHT in New Zealand appear to have sufficient independent control over data about FLYBEST passengers to come within the scope of the New Zealand law.

48. Individuals, including foreign nationals, have a range of entitlements under the Privacy Act. The Act has also created a comprehensive system of supervision, and enforcement through the Privacy Commissioner (lacking only a pro-active audit role), and an associated complaints review machinery. The New Zealand Privacy Commissioner has jurisdiction over the personal information held in New Zealand by all the airlines, whether domestic or international, and straightforward, cheap and easily accessible processes are available for individuals who allege a breach of one the privacy principles, with the prospect of effective remedies.

49. The only limitation on a non-resident's rights relative to a New Zealand citizen or permanent resident is that he or she cannot make an enforceable access or correction request from outside the country. If passenger data are revealed to third parties, both the Privacy Act and in some cases other laws limit the use that can be made of it. The absence of a comprehensive onward transfer provision in the law would only be an issue in this case study if personal information about European passengers were sent to a third country without their consent, and this seems unlikely.

50. Personal information about a European passenger flying in New Zealand with FLYBEST/JETWELL and with SOUTHFLIGHT is therefore protected by law in a way which in most significant respects meets the test of adequacy envisaged by the Article 29 Working Party in relation to Article 25 of the EU Directive.

51. The complaints backlog is disturbing. However, the important fact is that all of the airlines and other organisations handling data about international passengers in New Zealand are all liable under the Privacy Act for breaches of any of the Information Privacy Principles and that comprehensive and easily accessible remedies are available to a

passenger if his or her privacy is breached (with the exception of the limited access and correction rights).

Sensitive Data in Airline Reservations

(f) *United States of America*

The Nature and Circumstances of the Transfer

1. AIRINT AIRLINES is a major international carrier that operates flights between Europe and the United States. AIRINT has employees in the United States who service its passengers.

The Booking

2. A citizen of Eurostate, a country in the European Union (EU), books a flight on AIRINT from Euroville to Washington Dulles Airport located in the State of Virginia. The passenger then continues on to Indianapolis, Indiana, on LOCALAIR, a domestic United States carrier. The passenger returns to Euroville using the same airlines and flying through the same cities.

3. The passenger is a member of AIRINT's 'frequent-flyer' programme, and AIRINT knows from information provided previously that he will require a wheelchair at the airport and a kosher meal. This information is retrieved at the time of booking from the passenger profile using the passenger's frequent-flyer number.

4. Immediately before booking the LOCALAIR flight, the passenger connected from home to LOCALAIR's Internet website and joined its frequent-flyer programme through the LOCALAIR Internet website. For the portion of the flight on LOCALAIR, the LOCALAIR frequent-flyer number appears on the ticket.

5. The booking of a flight directly from the airline is one of four ways that international bookings might take place. Flights can be booked: 1) through a travel agent who will have access to international reservation systems such as Galileo or Sabre; 2) through AIRINT's Internet site; 3) using a toll-free number; or 4) in person at an AIRINT office. The origin of the booking has some subtle implications for how personal data are stored and transmitted (see 'Recommendation 1/98 on Airline Computerised Reservation Systems' from the EU's Article 29 Working Party). For this scenario, however, we assume that the booking is made directly through AIRINT's telephone sales department. AIRINT also handles the booking on LOCALAIR.

Personal Information Flows – Euroville-to-Washington Flight

6. When a flight is booked in Eurostate, a 'Passenger Name Record' (PNR) is created in AIRINT's Computerised Reservation System (CRS), the database for which is located in Eurostate. PNRs must contain a name, itinerary, telephone number, the ticketing option (i.e., by what date it must be paid for), and the name of the person who telephoned in the reservation. The fares and taxes payable are calculated automatically (taking account of any special fares) and the amount and method of payment will also be added in due course - if by credit card, the card type, number, expiry date and merchant authorisation code. The PNR would also hold the request for a special meal and a wheelchair, using internationally recognised codes issued by the International Air Traffic Authority (IATA). Permanent preferences registered with AIRINT's frequent-flyers club programme are transferred automatically from the club database into the CRS. Other codes entered on a one-time basis might indicate characteristics such as unaccompanied minor, prisoner, or special needs for passengers who are not club members. Seat allocations are generated in advance for First and Business Class passengers, club members and others with special needs, while seat allocations for most other Economy passengers are currently not made until check-in.

7. The PNR is held on AIRINT's mainframe computer in Euroville, to which authorised AIRINT personnel around the world would have access. Between 36 and 48 hours before departure, relevant fields from the PNR are transferred to the Departure Control System (DCS). DCS is a subsidiary database held in Eurostate but, like the CRS, accessible worldwide. The day before the flight, the check-in agents 'edit' the flight list to make sure there is the appropriate weight distribution, establish fuel requirements, order meals, and ascertain that those with special needs have been properly accommodated.

8. When a passenger checks in for the flight at Euroville Airport, the AIRINT check-in staff use the passenger's last name to access his record on the DCS. Check-in staff (whether employees or agents) can also access this information by seat number. At a pre-set time before departure (approximately 30 minutes), a complete list of passengers by seat number is printed and given to the cabin crew; any subsequent last-minute changes are notified separately.

9. The records for each flight are purged from the DCS some two hours after the flight has landed. Printed copies of all flight lists are held at Euroville Airport for 12 months.

10. The PNR itself is purged from the CRS between 24 and 48 hours after the completion of the last leg of each journey. It is, however, retained in a separate database for two years for the purpose of management analysis.

11. The AIRINT flight attendants know from the passenger list about special needs and will probably welcome the passenger by name. They will have be given his special meal request and will know that he needs a wheelchair in Washington.

12. Passengers arriving in the United States are required to complete immigration and customs forms upon arrival. In this case, the passenger clears immigration and customs at Washington Dulles. Information provided to the United States Immigration and Naturalization Service (INS) and to the United States Customs Service. Information provided to INS on form I-94 is maintained in several different record systems. One system is subject to the Privacy Act of 1974, a code of fair information practices for federal agencies. However, foreign nationals have no rights under that Act. Nevertheless, the Act does still impose some requirements on federal agencies that remain applicable, and foreign nationals can obtain access to records under the Freedom of Information Act. In addition, agencies sometimes grant some Privacy Act rights to foreign nationals as a matter of discretion. Information provided to the Customs Service is used only during the clearance process for individuals passing through customs. The information is stored in a warehouse for several years, but the information is only retrievable by flight number. The information does not qualify for protection under the federal Privacy Act of 1974, and it cannot be readily retrieved.

Personal Information Flows – Washington-to-Indianapolis Flight

13. At Washington Dulles airport, the passenger transfers to LOCALAIR, and the relevant details of the reservations are automatically transferred from the AIRINT CRS to the comparable LOCALAIR system. The details transferred would only be the relevant stage booking, the immediately-prior connecting flight and any special needs. 'Second' carriers do not have direct access to AIRINT's CRS and do not need, or receive, the complete journey details, booking contacts or PNR history.

14. On arrival in Indianapolis, the passenger leaves the airport by a hired car and proceeds to a hotel. The car company and the hotel can receive reservations directly through the LOCALAIR CRS, although the transfer of data would not convey special-needs information such as the use of a wheelchair.

Overview of the Regulatory Environment for This Case

15. There is currently no United States data protection office, either at state or federal level, with jurisdiction over the personal information held by the airlines, whether domestic or international.

16. As part of its general oversight of airline safety and operations, the United States Department of Transportation (DOT) could, in theory, conduct oversight of fair information practices. However, there is no evidence that the Department has shown any interest in fair information practices.

17. Airlines are members of a major trade association, IATA, which has headquarters in Montreal. International airline policy is co-ordinated by the International Civil Aviation Organisation. Airlines are members of a major trade association, IATA, which has headquarters in Montreal. International airline policy is co-ordinated by the International Civil Aviation Authority (ICAO), a United Nations-affiliated body located in Montreal. AIRINT and LOCALAIR are subject to the 1996 ICAO 'Code of Conduct for the Regulation and Operation of Computer Reservation Systems (CRS)'. Article 11 states that 'air carriers, system vendors, subscribers and other parties involved in air transportation are responsible for safeguarding the privacy of personal data included in the CRSs to which they have access, and may not release such data without the consent of the passenger.' The ICAO issues standards and recommended practices for both airlines and members states, but it has no enforcement powers.

18. American air carriers also are members of the Air Transport Association of America (ATA), but that association has not issued any privacy policies apart from security policies (see below). No American airlines or airline trade associations are members of any of the privacy self-regulatory associations.

Purpose Limitation, Transparency and Opposition

Collection

19. Most of the information recorded by AIRINT in a PNR is either provided by or on behalf of the passenger or is generated by AIRINT (e.g., the flight and seat numbers). The only information obtained from third parties would be authorisations for credit-card debits and the reference numbers returned from the CRSs of any other carriers involved in the journey.

20. The AIRINT 'Conditions of Carriage' declares that:

> 'The Passenger recognises that personal data has been given to Carrier for the purposes of making a reservation for carriage, for obtaining ancillary services, and for facilitating immigration and entry requirements. For these purposes, the Passenger authorises Carrier to retain such data and to transmit it to its own offices, other carriers or the providers of such services, in whatever country they may be located.'

It is not clear how, and in what manner, this assurance is made known to passengers.

21. The standard 'Conditions of Contract' used by LOCALAIR and other American air carriers and distributed with each ticket has no statement about the use, maintenance, or disclosure of personal information.

22. In Eurostate, and while the PNR is being accessed by AIRINT personnel in the United States, the collection and use of personal data will be in accord with policies set by Head Office in Eurostate. Company policy, worldwide, is guided by the requirements of the Eurostate data protection law. AIRINT representatives claim that the company’s data

protection policies are probably somewhat tighter than those of airlines operating in the United States. For a passenger originating in Eurostate, therefore, limits imposed for the collection of personal data are determined by the requirements of the Eurostate data protection law, as interpreted by company policy and communicated to employees.

Use and disclosure for AIRINT's purposes

23. The information AIRINT holds about passengers is used by the company, and by other organisations involved in the journey, for the purposes of providing travel and related services. These uses are not only within the reasonable expectation of the passenger but will generally be with at least their implied consent. Depending on whether the Conditions of Carriage cited above are drawn to their attention, this could be taken to be express consent, although the notice is neither visible nor detailed. While AIRINT itself is subject to the Eurostate data protection law, LOCALAIR and the American hotel and car-hire firms that necessarily receive personal information about the passenger are under no statutory obligation not to use that information for other purposes.

24. For passengers classified as entitled to 'special services', the AIRINT database holds a more complete profile of the passenger's flight history, hotel reservation and car-hire needs, frequent-flyer history, and other information. AIRINT personnel have complete access to these data to provide the 'personalised' service that such customers have come to expect. It should be noted, however, that AIRINT retains a separate database of its frequent-flyer passengers (including those receiving special services) in each country or region. Most other airlines retain central databases. For passengers from EU countries, the database is maintained in Europe and is subject to local data protection rules. Because there is currently no privacy law applying to general private sector activities in the United States, the only limits on the use of data about club members or other passengers are those in the United States contractor's own policy and in the terms of their contract with AIRINT.

Disclosure to third parties for other purposes

25. AIRINT employees in the United States will have been made aware through training, and through a notice on the computer access applications (see below), of the general policy about the disclosure of reservations information. They are reminded that: 'The carriage by air of passengers is a matter of private contract between the airline and the passenger concerned. As a general rule details of that contract should not be given to third parties particularly when the request is made on the telephone.' Employees are told not to disclose information about a passenger, including via the telephone, unless the information is given to:

- a colleague/another airline or agent for the purpose of reservation booking or ticket issue;
- the passenger himself and you have taken the necessary steps to ensure that this person is the passenger;
- some other person with clear passenger consent, and there is a record of this in the PNR;
- an appropriate person or organisation in an emergency to prevent injury or damage to someone's health.

26. Employees are also advised, orally, that requests from the police or law-enforcement bodies must be referred to the investigations unit, and those relating to legal proceedings to the legal department. They are also advised that details of medical conditions must not be disclosed without reference to the Senior Medical Officer.

27. AIRINT's personnel work, however, in a number of different settings that might guide the ways in which these rules are interpreted. In a telephone-sales context, they are quite strictly adhered to. If the person to whom the sales agent is speaking is not travelling, or is not mentioned in the contact field of the booking (such as the name of the secretary), then details cannot be given out.

28. In the airport environment, however, practices may differ. AIRINT staff and agents will have access to passenger information before, during and after a flight. A greater variety of more urgent requests arise within the airport context, in which requests might come from airport security personnel, State law-enforcement agencies, Customs agents, or Immigration officials.

29. Requests for personal information from authorities, whether at the airport or to AIRINT offices, will normally be handled by a supervisor. At the airport, requests from Customs or Police officers (usually known personally) are handled informally with no record being kept, unless there is a need for an accompanying 'statement' from an employee. Current policy in AIRINT offices is to ask for identification, and usually a faxed request, but not to enquire any further into the justification, or to try to impose any conditions on use or further disclosure. Request forms are filed but no indication is made on the PNR or Club database.

30. The major circumstances under which a passenger's records would be accessed after a flight would be if the passenger left a possession by the seat. If the flight attendant or cleaning crew found a possession, AIRINT staff would be able to access the PNR by seat number and contact the telephone number on the PNR (up to the time the PNR is deleted, after which the problem would be handled via Eurostate). LOCALAIR could be expected to have similar arrangements.

31. The deletion of passenger records from the computer system shortly after the completion of a flight should ensure that PNR data would not be available outside the company for any length of time. Third-party requests for access after the PNR has been archived would have to be made in writing and considered in Eurostate under data protection law.

32. In the United States, a passenger can sign up for AIRINT's frequent-flyer programme by telephone. Applicants are asked to provide name and address (home or business), length of residence in their city, home and business telephone numbers, birth date, seating preference, e-mail address, and passport number if available. No notice of information practice is provided over the telephone and no choices are offered. AIRINT's website offers information about its frequent-flyer programme, but there is no privacy notice or notice of information practices.

33. A passenger living in an EU country who joins LOCALAIR's frequent-flyer programme through the airline's Internet website is asked to provide name and address (home or business), home and business telephone numbers, company name, most frequent form of travel (business or leisure), and date of birth. An applicant is also presented with a tick-box that he is instructed to check to receive e-mail with important marketing messages from LOCALAIR. The passenger is informed that the e-mail address will be used only by LOCALAIR and its marketing partners and will not be shared with or sold to other companies. The tick-box is already checked (indicating willingness to receive e-mail) and the applicant must click on it to uncheck it. The box is prominently displayed in the online application. The notice does not describe who qualifies or may qualify as a 'marketing partner'.

34. A privacy notice available to a LOCALAIR frequent-flyer applicant through a weblink offers more information about information practices and options. The use-disclosure portion states that information provided will be used for marketing. This offers no more information than the tick-box. The privacy notice describes four separate opt-outs available to a frequent-flyer club member. The first permits opt-out for LOCALAIR e-mail marketing. The second relates to the availability of e-mail addresses to LOCALAIR marketing partners. A third relates to postal mailings from both LOCALAIR and its marketing partners. A fourth allows a passenger to prevent sharing of telephone numbers

with marketing partners. In all cases, choices are exercised by composing and sending an e-mail message to the webmaster of LOCALAIR's website. The e-mail message seeking opt-out must specify which of the choices the frequent-flyer member wishes to exercise. No form with tick-boxes is offered. The opt-out choices available through the privacy statement are more detailed than are described in the tick-box on the basic application form, but the process of opting-out is more difficult.

Data Quality and Proportionality

35. Given the central direction of AIRINT's personal-information policy and computer-systems design, any data collected in the United States are largely governed, indirectly, by the requirements of the Eurostate data protection law. Data are collected in order to fulfil the private contract between the carrier and the passenger concerned. The standard minimum amount of information needed for the creation of a PNR would seem necessary and not excessive to fulfil AIRINT's obligations; any further information supplied (about special needs) is presumably provided by or with the consent of the passenger. In the case of a round-trip booking made in Euroville, additional information obtained during the United States portion of the travel may be minimal in most cases.

36. Some information collected through the reservation system can be sensitive. Airlines may collect a variety of medical information: physical handicaps, diabetic status, allergic reactions, etc. Some passengers have special dietary needs: kosher meals, no salt, vegetarian, etc., which give clues to religious affiliation or medical conditions. International airlines might also receive other categories of sensitive data, including information on dignitaries, deportees, unaccompanied minors (who might be in the middle of a parental-custody dispute), and members of groups who have certain sensitive affiliations, such as some political movements. Some sensitive information is held permanently in the regional databases and this is reconciled daily with AIRINT's master Customer and Marketing database in Eurostate. Data-quality problems arise from this need for matching, although this will be reduced by the proposed introduction of a new uniform database serving both AIRINT itself and its contractors.

37. AIRINT employees are also advised, orally in training, to refrain from placing into the central database 'any information or statement about a passenger which may be inaccurate or disparaging or discredit the passenger in any way.' There appears to be no express 'passing on' of this guidance to LOCALAIR employees acting as AIRINT's agents, but LOCALAIR itself can be expected to have a similar policy and training in respect of their own passengers.

Security

38. Security requirements are also directed from Eurostate. None of the PNR data is encrypted. AIRINT's CRS, the DCS and the Customer and Marketing database are password-protected for all users - its own staff and check-in agents. There are different levels of access depending on status in the organisation. Employees, agents and contractors' staff needing access all have to complete an application form which also serves to remind them about the need for confidentiality. After endorsement by a supervisor as to the level of access required, the applications are processed in Eurostate and authorisation codes (user IDs) are issued. To access the system, users have to input their ID and a self-selected password (which has to be changed at regular intervals). The history of any changes to a PNR is recorded. There is an audit trail of all access to the CRS.

39. The ATA is the principal trade association for American air carriers, and it has issued recommended practices for providers of electronic airline reservation services. LOCALAIR is a member of ATA, but AIRINT is not. All passenger information that is not considered public information is considered to be 'sensitive' information and subject to the

ATA policy calling for acceptable data security during transmission and storage. The recommended information security policies call for use of encryption to accomplish both message privacy and message integrity. IATA has similar recommendations. Whether these recommendations are followed in practice could not be determined.

40. Physical security policies require airlines to make sure that they have adequately verified the identity of all passengers. The ATA policy reminds operators of electronic reservation systems that the Federal Aviation Administration (FAA) in the DOT may require the collection of additional information from passengers for security purposes. The specifics of FAA security requirements are not public, and neither the FAA nor the airlines will provide detailed information pertaining to security policies or practices. FAA rules expressly provide that security information is not public.

Access and Rectification

41. Access by passengers to personal information held about them by AIRINT tends to occur for practical and mundane reasons (such as checking schedules and preferences), and will normally take place before departure. These data can also be accessed formally via the 'subject access' provisions of the Eurostate data protection law, which enables European passengers to check the accuracy, relevance and completeness of information. It is difficult to envisage circumstances under which European passengers would want formally to access or correct their records during the very brief period while they are processed by AIRINT within the United States.

42. No United States law requires LOCALAIR to provide passengers or frequent-flyer members with a right to access or to correct records. The company has an interest in encouraging customers to keep address and telephone information accurate. Frequent flyer records are regularly sent to passengers who can correct or contest flight information. However, no LOCALAIR policy grants a general right of access or correction to all company personal records.

43. If either AIRINT or LOCALAIR lawfully gives information to a third party in the United States, access and correction rights would generally be dependent on the policies of that third party. Records disclosed to federal agencies would likely become subject to the Privacy Act of 1974, a statutory code of fair information practices that applies to federal agencies. However, applicability of that Act is dependent on actual practices for filing and retrieval of documents. Also, the Act grants no rights to foreign nationals, although access to federal records (but not correction) may still be possible under the Freedom of Information Act. Some states have privacy laws that might grant access and correction rights to data subjects, but access rights for law enforcement records are not common. In general, for disclosures to non-governmental entities, any rights granted a data subject would be determined by the entity. No omnibus federal or state privacy statute requires record keepers to offer access and correction rights to data subjects.

Onward Transfer Restrictions

44. AIRINT does not transfer personal information from PNR records to officials within other jurisdictions. If, for example, United States law-enforcement authorities were interested in a passenger list, then they would have to apply in writing to AIRINT's Eurostate officials. LOCALAIR is often co-operative with law enforcement for airport security purposes, but other requests by law-enforcement agencies for other purposes are handled on a case-by-case basis. Federal airline regulatory agencies can obtain access to passenger records, but access is rarely needed.

Remedies

45. AIRINT has an internal complaints-handling process. Most complaints relate to issues such as pricing and the flexibility of the tickets purchased, as well as to the flight experience. Complaints about breaches of the privacy principles are rare. Before the flight, complaints are handled through a hierarchy of service agents, managers and directors. If the complaint occurs after the flight is taken, it will be referred to the most appropriate branch of the Customer Relations Department. LOCALAIR also accepts and considers passenger complaints in a similar manner.

46. The DOT accepts complaints about air travel service problems. The complaint process focuses on delays, baggage handling, and oversales. Information available at the DOT website does not refer to privacy or information-policy complaints. In any event, the DOT mostly forwards complaints to the airline for 'further consideration'.

47. In theory, at least, passengers may be able to pursue legal remedies in American courts relying on contract or tort remedies. However, there appear to be no precedents for privacy actions against airlines. Whether a contract or tort action could be viable might depend on the specific terms of airline tariffs. It is possible that airlines have limited liability under their tariffs. Regardless, finding a legal theory for a privacy action when there are no statutory standards and probably no contractual standards would be difficult. Tort actions might have a better chance, but state rules vary considerably. No record of a lawsuit against an airline for breach of fair information practices could be found.

Accountability

48. Theoretically, AIRINT's employees, agents and sub-contractors in the United States. should be given exactly the same guidance about personal-information practices as their counterparts in Eurostate. Written policies, already cited, are disseminated in paper format and online. There is no privacy officer, designated as such, but security personnel assume broad responsibility for monitoring access to the central reservation system.

49. Because it is subject to the Eurostate data protection law, AIRINT is accountable for its personal information handling practices to the Data Protection Authority, which has a range of powers to ensure compliance if breaches of privacy or weaknesses in an organisation's systems are brought to its attention, although it does not have the power to conduct pro-active audits of compliance.

50. AIRINT is only subject to the Eurostate law in respect of data held (controlled) outside Eurostate if those data are intended to be used in Eurostate. In the circumstances of this case study, it seems clear that any data held on AIRINT's main computer systems would be subject to the Eurostate law, although it is arguable whether data about an international passenger held locally by AIRINT staff in the United States would be covered. However, since AIRINT chooses to apply the standards required by Eurostate law to all its operations worldwide, data held and processed in a third country, such as Australia in this case study, benefit from the overall protection and accountability, even where it has no legal force.

51. LOCALAIR offers its employees some guidance on the handling of personal information practices. However, because it is based in the United States and does not fall under general data protection rules, its privacy policies are not as complete as AIRINT's. LOCALAIR does not have a privacy officer, but it does maintain security over its reservation and other computer systems. Security is of greater concern to LOCALAIR than privacy.

Conclusions

52. For airlines like AIRINT, guided by a more established set of data protection standards within their 'home country' legislation, there should be little difference between practices in the United States and those in the home country, in this case, Eurostate.

53. For domestic carriers like LOCALAIR, data protection rules are much less stringent and less carefully followed. However, the available evidence cannot indicate the precise ways in which practices differ from those of their European counterparts. Airlines and their reservations systems maintain vast amounts of personal information, and there is increasing awareness of the potential uses of that information. Except perhaps for frequent-flyer programmes, where direct-marketing uses of member information is common, it does not appear that airlines are currently exploiting their personal information resources as much as some other American industries. In general, no American laws would prevent subsequent use of those resources for marketing or other purposes.

54. Information that originates in airline reservation systems and is routinely transferred for travel-related purposes (to hotels, car-hire companies, etc.) becomes part of entirely separate personal information systems maintained by separate companies. The degree of privacy protection for that information would have to be determined through a separate enquiry. However, the absence of any omnibus data protection laws in the United States means that data protection policies and practices, if any, would be determined by the data controller and not by any external standard. For the most part, the travel industry has not been a participant in privacy self-regulatory efforts in the United States.

55. Overall, airlines have some policies designed to protect the security and, to a lesser extent, the privacy of personal information. It is difficult to assess the ability of these policies to deliver a reasonable level of compliance, but there is some recognition of privacy concerns. In the case of airlines headquartered in EU countries and directly subject to data protection laws, protections for data subjects are present. In the United States, however, external standards or laws for privacy of passenger information do not exist. Data subjects can obtain access to, and correction of, at least some personal information held by airlines through frequent-flyer programs and perhaps elsewhere. Otherwise, general assistance for privacy matters is likely to be difficult to obtain, as there is no identifiable source of help or advice. Consumer remedies for privacy violations are difficult to identify, and lawsuits over fair information practices would be novel.

Conclusions on Sensitive Data in Airline Reservations

1. Compliance with fair information practices for the six transfers of sensitive and other data in connection with airline reservations is generally good, but the complexity of the flow of such data, and of the uses to which the data are put, make generalisations difficult. The cases demonstrate how a single transaction may generate multiple data-transfers to multiple players. Passengers with complex flight arrangements that also involve 'special' and other services may find that their data flow through regimes with markedly different levels of privacy protection.

2. Where the data are processed for flights on airlines established in the European Union, protections afforded by 'home country' law and incorporated into company policies and practices are likely to be satisfactory. Where legal protections exist in the third country, they help to provide 'seamless' protection of the privacy rights of passengers for at least some of the data that are involved.

3. For passengers whose flights originate in the European Union are continuing to further destinations on domestic carriers within or between third countries, protection depends heavily on laws and codes in those jurisdiction, and its adequacy is less certain. The variety of regulations, and their absence in some instances, need to be considered in any determination of adequacy. Hong Kong and New Zealand differ generally from the other third countries in that laws are in place which apply to personal data used by domestic or international transport companies and their associates. Elsewhere, the position is less clear, and may be less satisfactory, given the lack of attention to data protection by foreign-based carriers and the limitations on the rights of foreign nationals to remedies in respect of those data. The role of international aviation bodies may be potentially important in establishing rules and standards of privacy protection for the flow of data.

4. Protection for the often very sensitive data involved in airline reservations is particularly important. Data in the Passenger Name Record (PNR) may not pose particular problems for privacy protection, given the specific uses that are made of it and the limited duration of its existence. However, the picture is additionally complicated by the ancillary processing of flight-related personal information in the 'frequent flyer' programmes and other ground-based services on offer to passengers, such as hotel reservations and car-hire. Transparency, the adequacy of the notice given to programme members, and the protection of databases may vary across countries. Passengers' data enter the world of marketing with its pressures to use personal data more intensively, a domain that is less well regulated in many jurisdictions, including third countries. Further difficulties of this kind may arise where bookings are made through travel agents, although they were not included in the case scenarios.

5. An assessment of adequacy therefore requires careful examination of the extent to which private- and public-sector laws and codes govern airlines and their partners in those countries, as well as the actual extent of protection afforded by company policies and staff practices. There is considerable variety, and there may be consequently much variation in privacy protection. On-site investigations of compliance with laws or codes in airport or commercial environments is appropriate in assessing adequacy.

6. At an early point in the flow of data, the degree of transparency may be less than desirable. The 'Conditions of Carriage' for flights include a very unspecific statement authorising the use of data by the company, other carriers, and providers of other services anywhere in the world. Passengers are very unlikely to be aware that they have consented to this. Especially where passengers' data are particularly sensitive, this lack of transparency may have implications for the adequacy judgement in this category of data transfer.

Medical/Epidemiological Data

(a) *Australia*

The Nature and Circumstances of the Transfer

1. A citizen of a European Union (EU) country, travelling in Australia, is found unconscious and taken to a public hospital in Canberra (which shall be called the Capital Hospital). Hospital personnel find a card in her possession that indicates that the bearer is a diabetic. It provides a telephone number of her medical services back in the EU country. A doctor contacts the patient's doctor and obtains information about her health status, treatment history and other matters which are thought to be relevant, including the name and contact telephone number of her partner. The treating physician and other personnel who see the transferred information are mainly employees of the hospital, but tests are obtained from a private laboratory, and at one stage, the treating doctor seeks an opinion from a consultant specialist in Sydney. The information used in the treatment of the patient (including the results of blood tests) remains in a file in the hospital when the patient is discharged. At the patient's request, a copy of the treatment record is sent to her doctor in the EU.

2. Reciprocal agreements with some countries enable people from those countries to be treated as public patients. The European countries with reciprocal agreements as at May 1998 were the United Kingdom, Italy, Malta, Sweden, the Netherlands and Finland. Patients from these countries are eligible for 'free' public hospital treatment. In other cases the patient would be ineligible, and would be charged for the cost of treatment by the hospital; the doctors would charge her as a private patient. In that case, records of her treatment would be passed to her private health insurance fund in her home country to process payment of the hospital and doctors' bills.

3. This transfer provides an opportunity to test the adequacy of data protection afforded to hospital records in Australia. The transfer of personally identifiable health information in connection with treatment, while not a predictable event, occurs regularly.

Overview of the Regulatory Environment for This Case

4. A hospital located in any Australian State or Territory could have been chosen. Canberra was selected because it is the only Territory, to date, with a modern data protection statute devoted entirely to the protection of personal health information. The Health Records (Privacy and Access) Act of 1997 of the Australian Capital Territory (ACT) is the only Australian statute that covers health related information processed by a wide variety of individuals and organisations. These include all health service providers (including doctors, nurses, pharmacists, therapists, hospitals, and laboratories), who are subject to the law in relation to all 'health records'.

5. The ACT law also applies to 'personal health information' held by any other organisation including employers and insurance companies, non-government organisations (such as counselling services and charities), research foundations and private contractors (such as home care services). It also applies to public bodies (such as government departments), although they were already subject to very similar rules under the Commonwealth Privacy Act of 1988. For these agencies, including the Capital Hospital which admits the European patient, the new law supersedes and replaces the Privacy Act.

6. In all six Australian States and at the federal level, access and correction rights are available to individuals under freedom-of information legislation if their information is held by public bodies, but not if it is held by other individuals or organisations. The other jurisdiction - the Northern Territory - lacks even these rights.

7. The rights conferred under the legislation are not confined to residents of the ACT or of Australia. The law protects 'health records' and 'personal health information' about any identifiable individual, including overseas visitors.

8. The ACT, like all Australian jurisdictions, has other specific laws containing provisions for the confidentiality and disclosure of health information, as well as common-law duties of confidence owed by health-care professionals to their patients. For the most part, however, these laws relate to particular ACT government programmes, and deal only with security and confidentiality - protection against unauthorised disclosure. The passage of the 1997 Health Records law is explained in part by the perceived need to provide a wider range of privacy rights, including notice, limitations on authorised use and disclosure, and data quality requirements. A particular stimulus for the legislation was provided by a High Court decision in 1996 that ruled that patients had no common-law right to access medical records about themselves.

9. The Australian Medical Association (AMA) has a Code of Ethics for doctors. Clause 1.3.4 of the AMA's Code reads: 'Keep in confidence information derived from your patient, or from a colleague regarding your patient, and divulge it only with the patient's permission. Exceptions may arise where the health of others is at risk or you are required by order of a court to breach patient confidentiality.'

10. The Medical Board of the ACT recently published Policy Paper No. 05 titled 'Maintenance of Medical Records'. The Board would use the Paper as a standard if it were enquiring into the practice of a doctor and might make a finding of unsatisfactory conduct if the doctor did not act in accordance with the policy.

Purpose Limitation, Transparency and Opposition

Collection

11. Under the ACT law, the Capital Hospital admitting the European patient can only collect health information (from or about any patient) for lawful purposes and by lawful and fair means.

12. There are several provisions in the ACT law relating to notification, openness and transparency. Data-collectors are required to notify consumers about general record-keeping practices, and specifically about access rights (Principle 5). They are also required to notify individuals about: the purpose of collection, whether their provision of data is mandatory, the identity of people likely to have access, and, to the extent known, any onward-disclosure practices of third parties (Principle 2). In this case, since the patient was unconscious when the information was obtained from her 'home' medical service, it was not possible to inform her of these matters at the time of collection. The law allows for notification 'as soon as practicable'. These provisions appear to match those in Articles 10 and 11 of the Directive, except that there is no express requirement to inform persons of their rights of access and rectification.

13. There is another weakness in the notification provisions, in that while the leader of the treating team is required to tell the patient about the identity of team members (unless it is obvious), he or she is expressly not required to inform the patient of the identity even of the broad categories of people who may have access for management, funding or quality purposes. (Principles 2.2, 9.3 and 10.3). This exception would arguably appear to conflict with Articles 10 and 11, unless it was held that notification of disclosures for administrative purposes was not 'necessary to guarantee fair processing'.

Use and disclosure for treatment purposes

14. The ACT law permits the Capital Hospital and treating professionals to use the information about the patient for the purpose of providing health care, and for associated management, funding and quality-control purposes. The law expressly provides for the sharing of information amongst members of the 'treating team' (Principle 6). People receiving information for these purposes are, however, bound by the ACT law to limit their use to the purposes for which they are entitled to access. (Principle 10.4)

15. Organisations keeping health records may use personal health information only for the purpose for which it was collected or received, i.e., the treatment of the patient, or where:

- the consumer has consented to the use;
- use of the information is necessary to prevent or lessen a significant risk to the life or physical mental or emotional health of the consumer or someone else;
- the use of the information is required or authorised by law;
- the use is directly related to the purpose for which the information was obtained; or
- the use is related to the management, funding or quality of health services received by the consumer. (Principle 9)

Disclosure to third parties for other purposes

16. The restrictions on the disclosure of information (Principle 10) are worded in similar fashion to the use principle, but also contain an exception for disclosure to family members in emergencies (and one for transfers of records where a patient changes health-care provider or where the provider closes or merges). The same principle also limits the use and further disclosure of the information by those who receive it from the record-keeper.

17. There is currently no centralised record-keeping, either in the ACT health system or Australia-wide, of all health-care events, so details of the patient's treatment will not pass outside the Capital Hospital other than in connection with the patient's actual treatment - e.g., any tests carried out by external laboratories, or references to specialists outside the hospital itself. Information about patients would be passed to the Commonwealth Health Insurance Commission if they were from one of the countries with a reciprocal arrangement, but no overt identifiers would be sent.

18. Public hospitals in the ACT have since 1989 been subject to the Commonwealth Privacy Act which makes specific provision for disclosures, without consent, for the purposes of medical research. (s.95, Privacy Act 1988). This is subject to detailed rules for approval by institutional ethics committees (IECs), and additional safeguards. The new ACT law disapplies the Privacy Act to health records in the ACT, but it is intended to include equivalent provisions in Regulations to ensure that research is not hindered. This would be consistent with the express recognition of research in Article 6(1)(b) of the Directive.

19. In the circumstances of this case, the ACT law strikes a balance, allowing the uses and disclosures of information that are necessary for the patient's treatment, including liaison with her doctor in her home country and contact with her partner, but also placing strict limits on the way in which the information about her can be used, and who can receive it. There are also exceptions where use or disclosure for other public interests is expressly required or authorised by law. All these provisions appear consistent with those in Articles 7 and 14 of the Directive. Article 8 generally requires additional constraints on the processing of sensitive data including health information, but not where the data are being used for the purposes of health care and administration.

Data Quality and Proportionality

20. Under the ACT law, a collector must ensure that information is relevant, up-to-date and complete and is not unreasonably intrusive (Principle 3). Record-keepers must take reasonable steps to ensure that the information is accurate and up-to-date before use (Principle 8) and have a continuing obligation to take reasonable steps to ensure that a record is accurate, relevant, up-to-date, complete and not misleading (Principle 7). These provisions perform the same function as Article 6(c) and (d) of the Directive.

21. There is a requirement in the ACT law not to delete information from a health record unless it is in accordance with a programme of archival destruction (Principle 7). Under normal circumstances, the patient's records would be kept by the Capital Hospital for at least ten years after her last contact with the hospital. This would be in accordance with the hospital's own policy on destruction of records, which is currently based on practice in New South Wales (the State which surrounds the ACT). At present there is no statutory obligation on the hospital in relation to keeping or destroying records. This is unusual, since other states usually have public records legislation which applies to medical records. This situation is about to change. Regulations under the Health Records Act are currently being prepared which will specify minimum periods for keeping medical records. The regulations are not likely to change the practice at the hospital, but they will create a minimum standard for private practitioners who may currently use a variety of practices.

Security

22. Again, the source of obligations about security are found in the Health Records (Privacy and Access) Act. A record-keeper must take reasonable steps to protect the record against loss, unauthorised access, use or modification, or other misuse (Principle 4). They must also take reasonable steps to ensure that security is observed by anyone to whom they disclose information from the record. The Federal Privacy Commissioner has interpreted the similar provision in the Commonwealth Privacy Act as requiring record-keepers to build into the terms of any contract appropriate security (and other privacy) controls. Principle 4 of the ACT law would appear to perform the function set out in Article 17 of the Directive.

Access and Rectification

23. The ACT law singles out access to patient records for special attention, and provides comprehensive rights for consumers and mechanisms for the exercise of those rights (Part III). The European patient would be able, after her treatment, to obtain access to any of her health records that had been created by any of the health care providers who had been involved in her treatment, wherever they were located. Those in the ACT are directly required to provide access, while a health-care provider in another State (or overseas) is under a similar obligation as a result of a section of the ACT law which implies a term in all contracts. The patient would therefore have a legal right of access to records held for instance, by a specialist consultant doctor, or by a private laboratory in Sydney. (She would have an independent right of access to any public-sector provider records under the relevant State Freedom of Information law.)

24. Access under the ACT law is to both facts and opinions, and the grounds for denying access are strictly limited and can be challenged (see under Accountability). Record-keepers may make a reasonable charge for providing copies or explanations, but the right to inspect a health record and make notes must be free of charge.

25. A right to request amendment of a health record, by way of correction or addition, is provided as part of the data quality principle of the ACT law (Principle 7), along with mechanisms for dealing with disputes about the content.

26. The access and correction rights and mechanisms in the ACT law appear equivalent to those set out in Article 12 of the Directive, with the exception that there is no obligation on the record-keeper to notify any third parties about corrections (Article 12(c)).

Onward Transfer Restrictions

27. There are no provisions in the ACT Health Records (Privacy and Access) Act that expressly regulate the transfer of personal health information to other jurisdictions. However, in the context of most foreseeable transborder transfers, such as those associated with the treatment of the patient in this case, further disclosures would be subject to the general provisions of the law relating to disclosures, security and access discussed above. These have the effect of extending the use and disclosure limits, the security precautions and the access rights to anyone outside the ACT who obtains access to information about a patient. There may however be some difficulties in effectively investigating or enforcing these rights in the event of an alleged breach by an interstate or overseas third party (see below under Accountability).

28. Transfer outside the jurisdiction might also occur for the purpose of conducting health research. The definitions of both 'record' and 'personal information' in the ACT law exclude de-identified information. If it were proposed to disclose (or just use) *identifiable* information about the European patient for research, this would have either to be justified under the 'related purpose' or 'quality' exceptions of Principles 9 and 10, or with her informed consent.

Remedies

29. The ACT Health Records (Privacy and Access) Act provides for complaints about breaches of the Act to be made to the ACT Community and Health Services Complaints Commissioner, an independent statutory officer. Rather than providing a separate mechanism, the Act simply applies the provisions of the ACT Community and Health Services Complaints Act 1993. This regime, which can ultimately lead to a judicial enforcement of a determination, and which provides for compensation payments where applicable, appears to be equivalent to the standards set out in Articles 22 to 24 of the Directive.

30. Apart from doctors, some other health-care professionals are also subject to similar codes of ethics. Complaints about breaches of these codes can be taken up with statutory registration boards, which can impose sanctions. But apart from supporting the principle of non-disclosure, these codes do not otherwise deal with other privacy issues.

Accountability

31. There is no express legal requirement on hospitals or other health care providers in the ACT to designate a member of staff as responsible for privacy and access matters. There is also no reporting requirement. However, both the ACT Freedom of Information Act and the Commonwealth Privacy Act do contain reporting provisions that require, annually, certain records to be compiled and made publicly available, and these obligations apply to public sector health service providers including the Capital Hospital (although the extent to which the Privacy Act requirements no longer apply is still being resolved).

32. The ACT law also contains a number of offence provisions, including ones prohibiting the unlawful requiring of consent, unlawful destruction, alteration or removal of health records, and unlawfully requesting or obtaining health records.

33. At the Capital Hospital all salaried staff are subject to the Public Service Management Act and Standards. Section 9(p) of that Act deals with confidentiality. Visiting Medical Officers (VMOs) are employed on individual contracts. Each contract is unique, but all include a standard clause which requires the VMO to act in accordance with the AMA Code of Ethics (see above).

34. Other contractors may work at the hospital. Standard government contracts deal with confidentiality, but mainly in relation to 'commercial-in-confidence' matters. But if contractors have access to patient information, their activities would be covered by the Health Records Act.

35. There is no express provision in the ACT health privacy law for any pro-active monitoring of compliance, such as inspections or audits. However, a number of independent officials, including the ACT Community and Health Services Complaints Commissioner, the Privacy Commissioner, the Ombudsman, and the Auditor-General, have jurisdiction over some or all of the parties likely to be involved in medical treatment and the associated record-keeping. Article 24 of the Directive is sufficiently vague about the way in which implementation is to be ensured, so that the oversight role of these officials would seem adequate.

Conclusions

36. For transfers of personal data into the health care system in Canberra, the 1997 ACT Health Records (Privacy and Access) law appears to contain major privacy principles and accountability mechanisms equivalent to those set out in the EU Directive. It is arguably deficient in terms of a few minor provisions such as notification of access rights and the lack of a disposal requirement and may be stricter in terms of its provision for medical research (although these last two may soon be remedied).

37. However, the ACT, which contains less than two percent of the Australian population, stands out as the exception amongst the States and Territories. None of the States, nor the Northern Territory, has equivalent legislation, and the full range of privacy rights and remedies are only available where personal information is held by Commonwealth government agencies, which are subject to the Privacy Act 1988. Access and correction rights are available in all of the States under Freedom of Information laws.

38. For health records created and held within the ACT, the 1997 law provides comprehensive coverage. Although not involved in this case study, personal health information other than in the form of a health record is also protected by the law. This means that any organisation holding information about an individual's health, illness or disability, such as a health insurer or an employer, is subject to the law.

39. The overall assessment of health privacy protection in Australia is that it is very uneven. The ACT situation demonstrates how a comprehensive health privacy law can meet most of the standards which the EU prescribes for member states. But transfers to other States would expose the personal data to a range of privacy risks, and there would be no mechanisms for taking up a complaint (other than in relation to a breach of confidence) or obtaining a remedy.

Medical/Epidemiological Data

(b) *Canada*

The Nature and Circumstances of the Transfer

1. A citizen of a European Union (EU) country, travelling in Manitoba, is found unconscious and taken to a public hospital in Winnipeg, Manitoba. Hospital personnel find a card in her possession that indicates that the bearer is a diabetic. It provides a telephone number of her medical services back in the EU country. Hospital personnel contact her doctor and obtain more information about her health status, treatment history and the name of her closest relative. The treating physician and other personnel who see the transferred information are mainly employees of the hospital, but tests are obtained from a private laboratory, and at one stage, the treating doctor seeks an opinion from a consultant specialist in Winnipeg. The information used in the treatment of the patient (including the results of blood tests) remains in a file in the hospital when the patient is discharged. At the patient's request, a copy of the treatment record is sent to her doctor in the EU. Records of the treatment are also passed to her private health insurance fund in her home country to process payment of the hospital and doctors' bills.

2. This transfer provides an opportunity to test the adequacy of data protection afforded to hospital records in Canada. The transfer of personally identifiable health information in connection with treatment of a visitor, while not a predictable event, occurs regularly.

Overview of the Regulatory Environment for this Case

3. The provision and regulation of health care is a provincial responsibility within Canada. Therefore, a hospital located in any Canadian province could have been chosen. Manitoba was selected because it is the only province, to date, with a modern data protection statute devoted entirely to the protection of personal health information. The Personal Health Information Act (PHIA) of 1997 is the only Canadian statute that covers health related information processed by a wide variety of health care 'trustees'. These include all accredited health professionals (such as doctors, nurses, pharmacists, therapists), all health care facilities (including hospitals, personal-care homes, laboratories and research foundations), public bodies (government departments, schools, local governments, regional health authorities and the Manitoba Public Insurance Corporation), health services agencies, and certain private contractors (such as home care services).

4. The major organisations excluded from the reach of the law are third-party insurers and private employers. Nevertheless, the scope of the Manitoba health legislation is wider than that in any other Canadian province with the exception of Quebec. Other provinces will provide some protection to the extent that hospitals and government health agencies are covered by public sector privacy protection laws. The Manitoba law is, however, unique. The rights conferred under the legislation are not confined to residents of the province or of Canada.

5. Manitoba, like all jurisdictions, has a number of laws containing provisions for the confidentiality and disclosure of health information. For the most part, however, these laws relate to particular provincial government programmes, and contain only very vague obligations for the protection of personal information. The passage of the 1997 PHIA is explained in part by the perceived need (as stated in the preamble) to develop a 'consistent approach to personal information because many persons other than health professionals now obtain, use and disclose personal health information in different contexts and for different purposes.' Although other, more specific statutes and common-law protections might apply to the protection of patient records by hospitals, the major protections are

afforded by this new legislation. The passage of PHIA is also explained, in part, by the on-going initiative to develop an integrated health information network in the province to which a range of health agencies and institutions can be linked. The law recognises that 'clear and certain rules for the collection, use and disclosure of personal health information are an essential support for electronic health information systems that can improve both the quality of patient care and the management of health care resources.'

6. In other provinces, isolated provisions on confidentiality of information appear in a range of health-related statutes: Hospitals Acts, Child and Family Services Acts, Cancer Acts, Nursing Home Acts, Health Insurance Acts, Pharmacy Acts, Employment Standards Acts, Child Welfare Acts, Social Services Acts and so on. The doctor-patient duty of confidence also has a powerful and long-standing influence. Health codes of practice have also been developed to bolster these other protections, though none have any particular relevance in the Manitoba case. For example, the Canadian Medical Association circulated a privacy code in 1998 for adoption by a range of health-care providers. The new federal Bill C-54 might also have some applicability to the extent that health care information is used and disclosed as part of a commercial transaction.

7. The only Privacy Commissioners in Canada that currently have jurisdiction over hospitals are located in British Columbia and in Quebec; they also, of course, have other responsibilities and limited resources. In the former, hospitals are regulated under the public sector Freedom of Information and Protection of Privacy Act of 1993. Private physicians are also regulated through a legally enforceable code of conduct of 1997. In Quebec, the location of the record is somewhat irrelevant; here seamless protection is provided by the parallel operation of the 1982 public-sector and the 1993 private-sector legislation.

Purpose Limitation, Transparency and Opposition

Collection

8. The limits imposed on the collection of personal health information are derived explicitly from Part 3 of the PHIA. A trustee shall not collect personal health information about an individual unless: 'a) the information is collected for a lawful purpose connected with a function or activity of the trustee; and b) the collection of the information is necessary for that purpose.' Whenever possible, 'a trustee shall collect personal health information directly from the individual the information is about.' Exceptions to this obligation are provided when the individual has authorised another method, when collection from the individual could endanger his or her health or safety, when time and circumstances do not permit, when inaccurate information might be collected, or when another method of collection is authorised by another statute or court order. A trustee who collects personal health information from the individual shall, 'before it is collected, or as soon as practicable afterwards, take reasonable steps to inform the individual of the purpose for which the information is being collected.' In this patient’s case, we can assume that doctors in the Winnipeg hospital judged that receipt of the patient record from the doctor in Europe was necessary to protect her health and safety and because ‘time and circumstances' did not permit collection through any other means. These provisions have been guided by Articles 9 and 10 of the Directive, except that there is no express requirement to inform individuals of the possible recipients of the data, or to indicate rights of access and rectification.

Use by the hospital for its own purposes

9. A trustee may use personal health information only for the purpose for which it was collected or received, and shall not use it for another purpose unless:

a) the other purpose is directly related to the purpose for which the personal health information was collected or received;
b) the individual the personal health information is about has consented to the use;
c) use of the information is necessary to prevent a serious and immediate threat to the mental or physical safety of the individual the information is about or another individual, or public health or public safety;
d) the trustee is a public body or a health care facility and the personal information is used to deliver, monitor or evaluate a programme that relates to the provision of health care or payment of health care by the trustee, or for research and planning;
e) the purpose is one for which the information may be disclosed under section 22 (see below); or
f) use of the information is authorised by an enactment of Manitoba or Canada.

10. Again, we can assume that the disclosure is covered under c) and was necessary 'to prevent a serious and immediate threat to the mental or physical safety' of this traveller.

Disclosure to third parties for other purposes

11. The restrictions on the disclosure of information are worded in similar fashion. A trustee may disclose personal health information without the data subject's consent for a wider range of reasons:

a) to another health care professional (to the extent necessary to provide health care to the individual);
b) to any person if it is necessary to prevent a threat to the individual's of the public's health or safety;
c) for the purpose of contacting a relative or friend of an individual who is ill;
d) to a relative of a deceased individual;
e) for the purpose of peer review or discipline of health care professionals;
f) for health research purposes;
g) for programme evaluation, research or planning;
h) to a computerised health information network and database;
i) to a public body to the extent necessary to obtain payment for health care;
j) to a person carrying out audit or legal services for the trustee;
k) if required in anticipation of a civil or quasi-judicial proceeding;
l) if the information is needed to comply with a subpoena, warrant or court order;
m) for the purpose of a law enforcement investigation;
n) for the purpose of complying with an agreement entered into under an enactment of Manitoba or Canada; and
o) if authorised or required by an enactment of Manitoba or Canada.

12. In the circumstances of the hospitalised foreign traveller, the PHIA provides a certain leeway to disclose personal health information without the individual's consent. In this context, the treatment record might be sent to other health care professionals, to relatives and friends, or to the agency in the EU country to the extent necessary to obtain payment for the health care treatment in Winnipeg. Any laboratory tests also conducted will be disclosed to the Integrated Health Information Network, on the assumption that, under any recurrence of the problem, the health care provider will need access to any tests recently performed. However, these provisions do not cover the release of such information to a private insurance company, such as that insuring this person's travels.

13. The Act does not provide for an explicit right to object to any of the above disclosures (a-o). A trustee may also give out name, general health status, and location to 'any person' provided the disclosure is not 'contrary to the express request of the individual or his or her representative.' If, for example, the patient travelling is a person about whom there might be a certain amount of media interest (a celebrity or politician perhaps), the legislation would seem to authorise the provision of this basic information,

unless the individual has already objected to that disclosure, which he or she may not be in a physical or mental state to do.

Data Quality and Proportionality

14. A trustee shall collect only as much information as is 'reasonably necessary to accomplish the purpose for which it is collected.' Moreover, 'every use or disclosure by a trustee of personal health information must be limited to the minimum amount of information necessary to accomplish the purpose for which it is used or disclosed.' The law recognises that health information is inherently sensitive and that its confidentiality must be protected 'so that individuals are not afraid to seek health care or to disclose sensitive information to health professionals.' The inherent sensitivity of health information is also recognised in the CSA 'Model Code for the Protection of Personal Information'. Any organisation claiming to abide by that standard must obtain express consent (rather than implied consent) for the collection and release of such information. Both these provisins appear consistent with the requirements for processing ‘special categories of data’ in Article 8 of the Directive.

15. Requirements for accuracy are stated very briefly: 'Before using or disclosing personal health information, a trustee shall take reasonable steps to ensure that the information is accurate, up to date, complete and not misleading.' When a trustee makes a correction to information, it is obliged to notify any other trustee or person to whom the information has been disclosed of that correction, when practicable. These provisions are consistent with Article 6 of the Directive.

16. Disposal requirements are governed under Section 17 of the PHIA. A trustee is expected to establish a written policy on the destruction of records and shall ensure that personal health information is destroyed in a manner that protects the privacy of the individual the information is about. The trustee shall also keep a record of the individual whose personal information has been destroyed, the method of destruction and the person responsible for supervising the destruction. These requirements are currently being clarified by regulation.

Security

17. Again, the source of obligations about security are found in the PHIA. A trustee shall 'protect personal health information by adopting reasonable administrative, technical and physical safeguards that ensure the confidentiality, security, accuracy and integrity of the information.' This involves the implementation of controls that limit the persons who may access information, and ensure that the information can be used unless the person accessing it is verified as a legitimate user. Trustees are expected to implement specific safeguards for information recorded in electronic form. In determining the reasonableness of the security safeguards, the trustee is to take into account the degree of sensitivity of the personal health information to be protected. More detailed requirements for written security policies are spelled out in regulation. These provisions perform the same functions as Articles 16 and 17 of the Directive.

Access and Rectification

18. The individual has the right, under the PHIA, to 'examine and receive a copy of his or her personal information maintained by a trustee.' A trustee must respond to the request within 30 days and shall make 'every reasonable effort to assist an individual making a request and to respond without delay, openly, accurately and completely.' If the request is refused, the trustee shall give the specific reason under the legislation, which may be:

a) if the information could reasonably be expected to endanger the mental or physical health or the safety of the patient or another person;
b) if disclosure would reveal personal health information about another person;
c) if disclosure could identify a third party who supplied the information in confidence;
d) if the information was used for the purpose of peer review, professional discipline or standards assessment; and
e) if the information was compiled principally for use in a legal proceeding.

Trustees are expected to sever non-disclosable information as far as is practical. Trustees may charge a reasonable fee for accessing and copying personal health information, to be determined by regulation. Both the statement of rights and the derogations are consistent with Articles 12 and 13 of the Directive.

19. It should also be noted that there is a complicated interplay between the PHIA and the 1997 Freedom of Information and Protection and Privacy Act (FOIPPA). If a third party requests access to personal health information, then the governing statute is FOIPPA. All other requests should be handed under the PHIA.

20. Individuals also have the right to correct information that is inaccurate or incomplete. Trustees must respond within 30 days. If no correction is made, then the trustee shall permit the individual to file a concise statement of disagreement stating the correction requested and adding the statement to the record. The correction or statement of disagreement shall be communicated to any other trustee who may have received the same personal health information.

Onward Transfer Restrictions

21. There are no provisions in the PHIA that explicitly prohibit the transfer of personal health information to other jurisdictions. In the context of a transborder data flow, such as the case of the hospitalised European traveller, further disclosures would be regulated under the provisions of the PHIA discussed above. One might assume that any subsequent transfer of medical information from Manitoba back to the host country for purposes of payment would occur not only with her consent, but also her active encouragement. However, information related to her condition and treatment might find its way to other organisations in other jurisdictions by other means. Three other provisions might have a bearing on the onward transfer question.

22. First, if a health care facility uses another organisation for 'information management or information technology services', then the trustee must enter into a written agreement that provides for the protection of personal health information. Any information manager is obliged to comply with the provisions in the PHIA. But information provided under such agreements is still deemed to be 'maintained' by the trustee who is therefore liable (under the Manitoba law) for any breaches of security or other contraventions of the legislation, wherever they may occur.

23. A second onward transfer scenario might occur for the purpose of conducting health research. The disclosure may only take place if the research has been approved by the appropriate institutional research review committee. This body makes a judgement about the importance of the work, the safeguards for personal privacy, the necessity to obtain individual consent, and the procedures for anonymisation and record destruction. The PHIA does not apply to 'anonymous or statistical health information that does not, either by itself or when combined with other information available to the holder, permit individuals to be identified.'

24. The third provision that bears upon the question of onward transfers is that which prohibits the commercial sale of personal health information. An especially contentious issue in Canada at the moment is the collection and processing of health information from

pharmacy billing records in order to determine aggregate and individual prescribing patterns of Canadian physicians. These data are processed in the United States by an international health informatics company and then sold to pharmaceutical manufacturers for marketing purposes. All such data, however, are disclosed without patient identifiers. It remains an open question, beyond the scope of this analysis, whether a physician's prescribing behaviour is personal health information under this legislation.

Remedies

25. If a trustee were withholding personal health information unfairly or, for that matter, failing in any way to observe the Act, individuals (including non-citizens) may complain to the provincial Ombudsman, who is also responsible for oversight of the FOIPPA as well as to receive general complaints under the Ombudsman Act. The Ombudsman has general responsibility to:

a) conduct investigations and audits;
b) inform the public about the Act;
c) receive comments from the public;
d) comment on the implications of proposed legislative schemes or policies for the protection of personal health information;
e) comment on record linkage, and other technological applications;
f) consult with experts; and
g) engage in or commission research.

26. He is given broad powers to compel the production of records, to enter premises, and to report on the operation of the Act. The provincial Ombudsman has responsibility for overseeing compliance with the act and will handle complaints from individuals concerning their rights of access and the collection, use and disclosure of personal health information. He may also recommend that individuals be allowed to examine those portions of personal health information which the trustee has withheld.

27. If the trustee ignores the Ombudsman's recommendations or refuses to carry them out, individuals have a right to take the case to the Manitoba Court. The court has the power to order a trustee to allow the examination of information and obtain copies of the portions of personal health information that have been withheld. The act permits fines of up to CAN$50,000 a day against trustees for violating the act and may be imposed for every day that a violation continues. This fine applies to a variety of offences, including deliberately erasing or destroying personal health information to prevent someone from getting access to it; collecting, using, selling or disclosing personal health information in violation of the Act; and, failing to protect personal health information in a secure manner. The legislation makes no distinction between citizens and non-citizens with respect to the exercise of these rights.

Accountability

28. The Act stipulates that all health care facilities shall 'designate one or more of its employees as a privacy officer whose responsibilities include: a) dealing with requests from individuals who wish to examine and copy or to correct personal health information under this Act; and b) generally facilitating the trustee's compliance with this Act.'

29. Regulations under the Act direct trustees to implement a number of internal policies for the protection or privacy. First, trustees are expected to develop written security policies and procedures. Second, they must provide orientation and on-going training for their employees and agents. Third, all trustees shall ensure that 'each employee and agent signs a pledge of confidentiality that includes an acknowledgement that he or she is bound by the policy and procedures.' In addition, guidance notes have been issued by the Manitoba

Ministry of Health for both health facilities and health professionals. Regular staff training sessions are being implemented under the direction of Manitoba Health.

Conclusions

30. Personal information about Europeans receiving medical treatment in a Manitoba hospital is protected by law in a way which in most respects meets the test of adequacy envisaged in Article 25 of the EU Directive. While it is too early to assess of compliance with this legislation in practice, the PHIA appears to contain the major privacy principles contained within the EU Data Protection Directive and to provide an effective remedy, and appropriate assistance for data subjects (including those from overseas). It appears that serious efforts are being made to communicate to health care employees how the law should affect their work. Other provinces (including Alberta, Ontario and Saskatchewan) are currently considering the adoption of similar legislation.

31. The PHIA does not, however, provide 'seamless protection' for patient records even in Manitoba. Some of the heaviest users of personal health information (third-party insurers and private employees) are not covered by this law. The former would generally be subject to the voluntary code of practice from the Canadian Life and Health Association ('Right to Privacy Guidelines'). Breaches of privacy in the latter might be affected by a complicated patchwork of statutory and common-law safeguards.

32. It should also be stressed that the supervisory authority, the Manitoba Ombudsman, is a relatively small office with many other statutory responsibilities. It remains to be seen how the Ombudsman can fulfil the obligations under this law when he must also handle more general complaints resolution (under the Ombudsman Act), make judgements on access to information requests (under the FOI provisions of FOIPPA), and promote best privacy practices (under the privacy provisions of the same legislation).

33. Only in Quebec, is 'seamless protection' for health care records provided. Elsewhere, the adequacy of protection depends on the province to which the information is being sent and the type of recipient organisation. It is expected, however, that the development of integrated health information networks in other provinces will motivate the development of legislation similar to that in Manitoba. It is also expected that Bill C-54 might cover some commercial uses of personal health information. Until then, safeguards for health information in Canada will be very uneven.

Medical/Epidemiological Data

(c) *Hong Kong*

The Nature and Circumstances of the Transfer

1. A citizen of a European Union (EU) country, travelling in Hong Kong, is found unconscious and taken to a public hospital. Hospital personnel find a card in her possession that indicates that the bearer is a diabetic. It provides a telephone number of her medical services back in the EU country. Hospital personnel contact her doctor and obtain information about her health status, treatment history and other matters which are thought to be relevant, including the name and contact telephone number of her partner. The treating physician and other personnel who see the transferred information are mainly employees of the hospital, but tests are obtained from a private laboratory, and at one stage, the treating doctor seeks an opinion from a consultant specialist. The information used in the treatment of the patient (including the results of blood tests) remains in a file in the hospital when the patient is discharged. At the patient's request, a copy of the treatment record is sent to her doctor in the EU. Records of the treatment are also passed to her private health insurance fund in her home country to assist her in reclaiming payment of the hospital and doctors' bills. Before commencing her journey, the patient had purchased extra medical insurance from a private insurance company for the duration of her trip. There is no reciprocal arrangement between Hong Kong and the patient's home country for free care.

2. This transfer provides an opportunity to test the adequacy of data protection afforded to hospital records in Hong Kong. The transfer of personally identifiable health information in connection with treatment for foreign visitors, while not a predictable event, occurs regularly.

Overview of the Regulatory Environment for This Case

3. All hospitals and health care providers in Hong Kong are subject to the Personal Data (Privacy) Ordinance, passed in 1995. The Ordinance is a comprehensive data protection law covering both the private and public sector, and establishing the Office of the Privacy Commissioner for Personal Data to administer and enforce the law. The main data user in this case would be the Hospital Authority (HA), which manages and controls the public hospitals and public health care system in Hong Kong. The HA has issued guidance for staff on the operation of the Privacy Ordinance. Some of the specialist health care professionals from the private sector involved in treating the patient in this case may be data users in their own right.

4. The rights conferred under the Ordinance are not confined to residents of Hong Kong. The law protects personal information, including any health information, about any identifiable living individual - including overseas visitors.

5. Aside from the Ordinance, some health care professionals in Hong Kong are subject to strict professional discipline. The Professional Code and Conducts issued by the Hong Kong Medical Council includes a commitment to confidentiality. The Code defines as an 'abuse of professional confidence' disclosure of information obtained in confidence from or about a patient without proper justification. The effectiveness of this provision does, however, depend on how 'obtained in confidence' and 'proper justification' are interpreted. In Hong Kong law, there is a common-law duty of confidence by health care professionals to their patients. Common-law jurisprudence has tended to interpret 'obtained in confidence' narrowly and 'proper justification' quite broadly, with exceptions recognised for a range of other public and private interests. The common-law duty has to be considered alongside the statutory requirements of the Ordinance in deciding what limits are placed on disclosure of personal data; in different circumstances, either common law or legislation

could provide the 'tougher' restriction. But apart from supporting the principle of non-disclosure, these codes do not otherwise deal with other privacy issues.

Purpose Limitation, Transparency and Opposition

Collection

6. Under the Hong Kong Privacy Ordinance, the hospital admitting the European visitor can only collect personal data for a lawful purpose and by lawful and fair means, and where the collection is necessary for or directly related to the purpose (Data Protection Principle (DPP) 1). This should not pose any difficulty to the hospital in obtaining the information about the patient from her 'home' doctor in Europe.

7. There are several provisions in the Hong Kong Privacy Ordinance relating to notification, openness and transparency. DPP1 requires a data user to ensure that individuals from whom data are collected are informed about purposes, likely disclosures, access and correction rights and whether giving the information is mandatory or voluntary. These provisions appear to match those in Articles 10 and 11 of the Directive.

8. However, in this case, where the personal data are obtained from a third party (the patient's doctor) and she is unable to give consent, there is no requirement under the Hong Kong Ordinance subsequently to give her any information, although DPP5 obliges data users (the hospital in this case) to make available general information about personal data practices. The HA notifies its patients through a Notice to Patients posted in prominent positions and/or given to patients on admission.

Use and disclosure for health care and related purposes

9. Organisations controlling personal data (data users/controllers) may use those data only for the purpose for which they were collected or received, or a directly related purpose, or with the individual's prescribed consent (DPP3). There is no exception that deals expressly with health care, other than in a limited 'serious harm' situation (see below). However, most of the uses and disclosures of information that would be necessary for the patient's treatment, and associated administration, would almost certainly be seen as 'directly related' in terms of DPP3. This includes the storage of some information in a Patient Master Index. The Notice to Patients mentioned above in any event includes treatment, research and education as purposes of collection.

10. Information about the patient's treatment would not normally pass outside the hospital or hospital authority other than in connection with her actual treatment - e.g., the tests carried out by external laboratories or the reference to the specialist consultant outside the hospital itself (if these are required), or to relatives, if this is seen to be in the patient's interests. Both the private laboratory and the specialist consultant, if they are in Hong Kong, will themselves be subject to the Privacy Ordinance.

11. The use limitation provisions of the Ordinance appear consistent with those in Articles 7 and 14 of the Directive. Article 8 generally requires additional constraints on the processing of sensitive data including health information, but not where the data are being used for the purposes of health care and administration.

Disclosure to third parties for other purposes

12. Under the Privacy Ordinance, additional exceptions to the use (disclosure) limitation principle (DPP3) include (paraphrased):

- where the data are held by or for the government for security, defence or international relations and DPP3 would prejudice one of those matters;
- where the data are used for law enforcement and revenue purposes and there is a risk of prejudicing those purposes, for preventing or addressing unlawful or seriously improper conduct, or for preventing significant financial loss;
- where the use of (health information only) is necessary to prevent serious harm to the physical or mental health of the data subject or someone else. (Part VIII)

13. Note that there is no general 'required or authorised by law' exception. There are however specific exceptions, subject to certain conditions, for both statistics and research and for the news media, which could well apply to the patient's data. The news exception (s.61) is quite detailed and is supplemented in the case of health care by an 'arrangement', developed and published in May 1997 by the HA, Government Information Services, and the Office of the Privacy Commissioner. This explains that the HA may disclose to the news media, on the advice of the Information Service and without consent, the general condition (e.g., critical, stable) of people injured in major events, accidents (such as traffic accidents) or incidents (such as gang fights), and subsequent updates on their general condition.

Data Quality and Proportionality

14. A data user in Hong Kong must take practical steps to ensure that information is accurate (DPP2). 'Inaccurate' is defined as incorrect, misleading, incomplete or obsolete. The Ordinance is silent about other aspects of quality such as timeliness, completeness and relevance, although DPP1 requires collection to be adequate but not excessive for purpose. These provisions together perform substantially the same function as Article 6(c) and (d) of the Directive.

15. The EU Directive defines health data as one of the 'special categories' of Data (Article 8). The Hong Kong Ordinance provides no additional protection for these data. However, the Directive itself exempts the provision and management of health care from the processing prohibition (Article 8(3)).

16. DPP2 includes a requirement that personal data not be kept for any longer than is necessary, and this is backed up by s.26. These provisions are consistent with Article 6(e) of the Directive. Under normal circumstances, the patient's records would be kept by the Hong Kong hospital for several years - the HA has a records management, archiving and disposal regime which takes account of treatment, research and legal factors.

Security

17. Again, the source of obligations about security are found in the Personal Data (Privacy) Ordinance. A data user must take practicable steps to protect the record against loss, unauthorised or accidental access, processing, erasure or other use (DPP4). This principle performs the same function set out in Article 17 of the Directive.

18. The Hospital Authority has comprehensive security policies and practices covering both physical and logical access to manual and computerised data.

Access and Rectification

19. The Hong Kong Privacy Ordinance provides for individuals to have access to personal data held about themselves, and to be able to request corrections, through an obligation on data users (DPP6 and Part V). The European visitor would be able, after her

treatment, to obtain access to any information that was held by any of the data users involved in her treatment.

20. Access under the Hong Kong Ordinance is to both facts and opinions, and the grounds for denying access and refusing to correct information are strictly limited (set out in Part VIII of the Ordinance) and can be challenged (see below under Accountability). Data users may charge a reasonable fee for complying with an access request.

21. The access and correction rights and mechanisms in the Hong Kong law appear equivalent to those set out in Article 12 of the Directive, and there is also an obligation on the record-keeper to take practicable steps to notify any third parties who had received data within the preceding 12 months about corrections (s.23(1)(c); see EU Directive Article 12(c)).

22. The Hong Kong HA has established procedures for handling access and correction requests in compliance with the requirements of the Ordinance.

Onward Transfer Restrictions

23. Section 33 of the Hong Kong Ordinance will restrict data users from transferring personal data outside Hong Kong unless certain conditions are met, with the aim of ensuring that the data will continue to be protected and handled in accordance with privacy principles. This Section is not yet in force. The Privacy Commissioner has issued further guidance on this provision (Fact Sheet 1, May 1997).

24. When s.33 is brought into force, data users such as the HA will be able freely to transfer data to any places which have been specified by the Privacy Commissioner as having similar laws, without any further steps. It seems likely that EU member states will be declared to have similar laws, and therefore transfers about the European patient back to her home country will not pose any difficulty. But if the hospital wants to transfer information about her to a 'third country' which has not been specified, it will only be able to do so if:

- it has reasonable grounds for believing that there is a similar law in force (in the absence of any guidance from the Privacy Commissioner);
- it has obtained the patient's consent in writing;
- it is in her interests but in circumstances where consent is impracticable to obtain (but likely);
- the use or disclosure involved is an exempt one for the purposes of DPP3; or
- the data user has taken reasonable precautions and exercised 'all due diligence' to ensure the data will be handled responsibly.

Fact Sheet 1 suggests that one way of demonstrating 'due diligence' is to use contract terms, and a model contract is included.

25. If there were a need to transfer personal data about the patient to a 'third country' - perhaps for an opinion from a specialist doctor - in the course of treatment, then one or other of the first two exceptions would be likely to apply.

26. The inclusion in the Hong Kong law of an 'onward transfer' provision, similar in terms and effect to Articles 25 and 26 of the EU Directive, would appear to satisfy one of the core requirements which EU members are likely to require in order to assess a place as having adequate protection, once s.33 is in force. The breadth of the DPP3 exemptions as applied to s.33 would seem at first sight to weaken the effectiveness of s.33 as a safeguard, but are in fact analogous to the exception provided by Article 26(1)(d) of the Directive.

Remedies

27. The HA has an established internal process for handling complaints and seeking to resolve them.

28. Under the Hong Kong Privacy Ordinance, individuals can complain to the Privacy Commissioner about alleged breaches of any of the privacy principles. This right applies to any individuals about whom data are held; they do not have to be Hong Kong citizens or even residents. A temporarily resident or visiting foreign national would clearly enjoy all the rights given to individuals under the Ordinance.

29. The Commissioner's staff can assist the complainant and try to mediate. If this is unsuccessful, an investigation can lead to the Commissioner's issuing an enforcement notice, directing the data user to take specified action, and/or instigating prosecution. Contravention of an enforcement notice is an offence which can result in a fine or imprisonment. The Ordinance creates a right of action for compensation for damage or distress, although individuals would have to bring such action in the civil courts. Some privacy breaches may, of course, also be breaches or offences under other laws, and other remedies and penalties may apply.

30. Complaints about breaches of the Hong Kong Medical Council Code can be taken up with statutory registration boards, which can impose sanctions.

Accountability

31. The Hong Kong Ordinance provides for a scheme of data-user returns to be introduced by the Commissioner, which could include nomination of a person to receive access requests. There are no current plans to commence this requirement for any classes of data user. However, it is implicit in the notice requirements of DPP1(3) that data-users need to designate a member of staff as responsible for privacy and access matters, and the HA has done so.

32. The HA has an internal audit program which regularly addresses confidentiality and security safeguards, and from time to time includes auditing of compliance with other pertinent laws and regulations, including the other Data Protection Principles.

33. The Privacy Commissioner also has a pro-active monitoring role under the Ordinance and proposes to commence a programme of inspections (audits) later in 1998.

Conclusions

34. For transfers of personal data into the health care system in Hong Kong, the 1995 Personal Data (Privacy) Ordinance appears to contain both privacy principles and accountability mechanisms equivalent to those set out in the EU Directive. The law applies comprehensively to all organisations in both the private and the public sector, and the rights granted by the Ordinance apply to all individuals including foreign visitors.

35. Once the onward transfer provisions of s.33 are in force, the privacy protection regime in Hong Kong as it applies to the handling of medical information by a hospital would appear to meet all the main requirements that have been suggested as necessary to be assessed as 'adequate' for the purposes of Article 25.

Medical/Epidemiological Data

(d) *Japan*

The Nature and Circumstances of the Transfer

1. A citizen of a European Union (EU) country, travelling in Japan, is found unconscious and taken to a hospital. Hospital personnel find a card in her possession that indicates that the bearer is a diabetic. It provides a telephone number of her medical services back in the EU country. Hospital personnel contact her doctor and obtain more information about her health status, treatment history and the name of her closest relative. The treating physician and other personnel who see the transferred information are mainly employees of the hospital, but tests are obtained from a private laboratory, and at one stage, the treating doctor seeks an opinion from a consultant specialist in Tokyo. The information used in the treatment of the patient remains in a file in the hospital when the patient is discharged. At the patient's request, a copy of the treatment record is sent to her doctor in the EU. Records of the treatment are also passed to her private health insurance fund in his home country to process payment of the hospital and doctors' bills.

2. This transfer provides an opportunity to test the adequacy of data protection afforded to hospital records in Japan. The transfer of personally identifiable health information in connection with treatment of a visitor, while not a predictable event, occurs regularly.

Overview of the Regulatory Environment for this Case

3. The location of the hospital in this case has not been specified deliberately to avoid conveying an unrepresentative picture of the protection of medical records in Japan. The regulatory picture is very complicated; protection of medical information is obviously contingent on a multitude of local practices and specific ordinances. Only a general overview can be presented here.

4. Most hospitals in Japan are privately owned and operated by the doctors themselves. Most doctors also own the pharmacies attached to hospitals and clinics, but there are a smaller number of large public hospitals. A national system of health finances the Japanese health-care system.

5. There are on-going discussions within the Ministry of Health and Welfare about patient privacy issues, with few tangible results. However, there are a large number of ordinances at the prefectural, municipal and local level. About 42% (over 1400) of all local governments throughout the country have data protection ordinances in place. Typically, these only apply to the records held by local public-sector bodies, and most of them only apply to computer-processed personal data. It appears that none of these ordinances has yet been translated into English.

6. By and large, most local, municipal and prefectural data protection ordinances do not extend to the private sector; in Japan, hospitals are largely within the private sector. One exception is the prefecture of Kanagawa, which enacted a general data protection ordinance that covered both public- and private-sector institutions ('Ordinance on the Protection of Personal Data', Ordinance No. 6, March 30, 1990).

7. Self-regulatory initiatives on health information privacy also appear to be absent from the Japanese landscape. No specific sectoral code of practice for health care is being drafted pursuant to the 1997 Ministry of Trade and Industry guidelines. National and prefectural medical association have a number of rules for its members; none appears to extend to privacy protection.

Purpose Limitation, Transparency and Opposition

Collection

8. The usual procedure for a first out-patient visit to a large hospital involves patients filling in an application form and presenting it with their health insurance card at the reception desk. A 'registration card', which usually resembles a credit card, is issued, and a chart is prepared. These are taken to the relevant department where, in some cases, a number is assigned to indicate the patient's turn for consultation.

9. For Japanese patients, evidence of consultation is normally provided to the Ministry of Health and Welfare for the payment of state health insurance. These data are protected by the national 'Act for Protection of Computer Processed Personal Data held by Administrative Organs' (Act No. 95 of 1988). This legislation relies on a registration process for computerised files with the Management and Co-ordination Agency in the Prime Minister's Office. It is not clear whether the records of a foreign national, travelling on international travellers' insurance, would also have to be submitted.

Use by the hospital for its own purposes

10. The use of personal health information is also subject to few, if any, external controls. Most Japanese hospitals are not heavily networked, and proposals for health information networks are in a very fledgling state. There seems to be little pressure, at the moment, to find new uses for patient records.

Disclosure to third parties for other purposes

11. To the extent that there is any control on the disclosure of patient records, it is provided by a provision in the Penal Code requiring doctors and other professionals to keep confidential all data they obtain in the performance of their professional duties. Such information is considered privileged, and doctors have recognised a duty of confidentiality. Penal sanctions are provided for those who leak confidential information.

Data Quality and Proportionality

12. No legal or self-regulatory provisions mandates data quality or accuracy. There are no externally imposed limitations for retention. Practices presumably differ very widely.

Security

13. No legal or self-regulatory mechanisms mandate security provisions. The duty of confidence, stated above, prohibits the intentional leaking of personal health information. No sanctions apply to inadvertent or accidental loss or disclosure.

Access and Rectification

14. In June 1997, the Ministry of Health and Welfare released a policy which simply states that if a patient or a patient's family member requests a medical report, the doctor must provide it. Japanese doctors have traditionally not told patients when they are terminally ill, the theory being that disclosure would cause desperation and a rapid deterioration of the patient's condition; a recent *cause célèbre* has motivated a change in policy. It should be noted, however, that this policy does not grant a right to see the record itself, nor to insist on its correction if errors are found.

Onward Transfer Restrictions

15. No provision in any Japanese law prevents the transfer of health records to other jurisdictions, beyond the basic doctor/patient duty of confidentiality.

Remedies

16. There is no readily accessible mechanism for the resolution of complaints about personal health information practices. Breaches of confidence could be taken to the courts. But the contemplation of remedies for the mistreatment of personal health information is foreign to the Japanese political culture, for reasons given in the case on Human Resources data elsewhere in this Report.

Accountability

17. It has not been possible to analyse the personal information-handling practices of any health-care facility in Japan. Therefore, So no inference can be made about general levels of protection beyond the obvious conclusion that experiences vary widely. If there are any professional codes of practice or guidelines instructing hospitals as to their duties of care, they appear to be unavailable. It can be assumed that persons performing the function of privacy protection officer are a rarity.

Conclusions

18. In the absence of further information on compliance with data protection standards within Japanese hospitals, the initial conclusion must be that the protection of patient records in Japan meets few, if any, of the tests of adequate protection under the EU Directive. The assessment is more promising for public health care facilities, which might be controlled under the multitude of local, prefectural and municipal data protection ordinances.

19. The medical case points up the low salience of the concept of privacy within Japanese political culture. Anecdotal reports suggest that the lack of privacy is commonly experienced in Japanese medical facilities, from the proximity of hospital beds to a lack of confidentiality during consultations.

21. There is no commonly used Japanese word for 'privacy'. The contemporary literature uses the English word 'privacy' written in *katakana*, the Japanese script used for borrowed words. It is this concept that has recently entered Japanese law as a way to limit excessive intrusions. The terms 'privacy protection' or 'data protection' simply do not exist.

22. As with the other Japanese cases, these conclusions should be understood within the context of very different society and culture, in which the individualistic assertion of rights and interests is not part of the everyday world. Japanese legal institutions are designed to resolve and conciliate disputes, rather than to redress wrongs and grant remedies. Therefore, outsiders should be cautious about making judgements concerning the adequacy of Japanese law and institutions. The values that are expressed in the EU Directive may very well be embraced by some very different concepts, and implemented through different institutions that are difficult to compare in functional terms with those in Western societies. However, in terms of privacy protection for the data of European

citizens in Japan, there are a number of deficiencies of compliance with the principles of data protection as understood by the EU Directive, as well of redress and help.

Medical/Epidemiological Data

(e) *New Zealand*

The Nature and Circumstances of the Transfer

1. A European Union (EU) citizen, travelling in New Zealand, is found unconscious and taken to the General (public) hospital in the nearest city. Hospital personnel find a card in his possession that indicates that the bearer is a diabetic. It provides a telephone number of his medical services back in the EU country. Hospital personnel contact his doctor and obtain information about his health status, treatment history and other matters which are thought to be relevant, including the name and contact telephone number of his partner. The treating physician and other personnel who see the transferred information are mainly employees of the hospital, but tests are obtained from a private laboratory, and at one stage, the treating doctor seeks an opinion from a consultant specialist in New Zealand. The information used in the treatment of the patient remains in a file in the hospital when the patient is discharged. At the patient's request, a copy of the treatment record is sent to his personal doctor in the EU. Records of the treatment are also passed to his private health insurance fund in his home country to process payment of the hospital and doctors' bills.

2. This scenario provides an opportunity to test the adequacy of data protection afforded to hospital records in New Zealand. The transfer of personally identifiable health information in connection with treatment of overseas visitors, while not a predictable event, occurs regularly.

Overview of the Regulatory Environment in This Case

3. The New Zealand Privacy Act 1993 applies to the handling of personal information by all individuals and organisations (known as agencies) in New Zealand, whether in the private or public sectors. There is also a Code of Practice for Health Information issued under the Privacy Act, which in some respects substitutes for the general Information Privacy Principles in the Act, applying them more specifically in a health context. The Code has been drafted to be a complete substitute for the Act's Information Privacy Principles; the Act's 'principles' become 'rules' in the code, even where they are identical. The Code applies to health agencies, which include both public hospitals and individual health care professionals.

4. The rights conferred under the Privacy Act are not confined to residents of New Zealand. The law protects personal health information about any identifiable individual, including overseas visitors, although they only enjoy access and correction rights while they are in the country.

5. New Zealand has other specific laws containing provisions for the confidentiality and disclosure of health information, as well as common law duties of confidence by health care professionals to their patients. For the most part, however, these laws deal only with security and confidentiality - protection against unauthorised disclosure, and the other statutes relate to particular government programs.

6. The New Zealand Medical Association (NZMA) has a Code of Ethics for doctors which states that they are required 'to protect the patient's secrets'. A supplementary Guide to Ethical Behaviour includes the provision, 'Keep in confidence information derived from a patient, or from a colleague concerning a patient, and divulge it only with the permission of the patient except where the law requires otherwise.' Some other health professions have similar codes.

7. There is also a statutory Health and Disability Commissioner who administers a Code of Health and Disability Services Consumers' Rights. The Code includes a requirement to respect consumers' privacy although matters which can be the subject of complaint under the Privacy Act are reserved to be handled under that Act.

Purpose Limitation, Transparency and Opposition

Collection

8. Under the New Zealand Health Information Code, a hospital admitting a patient can only collect health information for lawful purposes and where the collection is necessary for that purpose (Rule 1). There is a presumption that health information be collected directly from individuals, with a range of exceptions (Rule 2) and by lawful and fair means (Rule 4).

9. Rule 3 requires the hospital to ensure that individuals are aware of a range of matters, including the right of access and correction. In this case, since the patient was unconscious when the information was obtained from his 'home' medical service, it was not possible to inform his of these matters at the time of collection (and technically not necessary as it was collection from a third party). The Code allows for notification 'as soon as practicable' afterwards (Rule 3(2)), and in this case it is likely that hospital staff would verify some information with the patient once he regained consciousness and he could be notified in accordance with Rule 3 at that time.

Use by the hospital for its own purposes

10. Organisations keeping health records (health agencies) may use personal health information only for the purpose for which it was obtained, i.e., the treatment of the patient, for a directly related purpose, or where:

- the individual or a representative has authorised the other purpose;
- the source is a publicly available publication;
- use of the information is necessary to prevent or lessen a serious or imminent threat to the life or health of any person or to public health or safety;
- the information is used for statistical or research purposes and not published in identifiable form
- use is necessary to avoid prejudice to a range of law enforcement and revenue protection functions;
- use is necessary for court or tribunal proceedings;
- the use is authorised by the Privacy Commissioner.

(Rule 10, paraphrased)

11. In commentary on the Health Information Code, the Commissioner has explained that in relation to the care and treatment of patients, 'directly related' purposes include health administration, including billing, auditing and service planning; training and education and monitoring quality. All of the uses to which the hospital would need to put the information received from Europe about the patient would be expected to fall within one of these purposes.

Disclosure to third parties for other purposes

12. The limits on the permitted disclosure of information (Rule 11) are worded in similar fashion to Rule 10, but also contain exceptions for disclosure:

- in general terms about a patient's progress when it has not been expressly ruled out by the individual or his/her representative (designed partly to facilitate media reporting of

accidents, and partly for disclosure to an individual's caregiver or near relative in accordance with recognised professional practice);
- to facilitate the sale or transfer of a health care business.

13. The Rule emphasises that in relation to many of the exceptions, only the minimum necessary amount of information should be disclosed, and that some of them apply only where the patient's authorisation is impracticable or undesirable. The Commissioner's commentary also emphasises that just because an exception might apply, a health agency is not required to disclose (other than where required by law); the decision to disclose remains a discretionary one and should be guided by ethical codes and common-law duties of confidence which in some circumstances may be more restrictive than Rule 11.

14. In the circumstances of this case, the New Zealand law strikes a balance, allowing the uses and disclosures of information that are necessary for the patient's treatment, including liaison with his doctor in his home country and contact with his family, but also placing strict limits on the way in which the information about him can be used, and who can receive it.

15. Personal information about the patient obtained from his health care provider in Europe might pass outside the hospital in connection with his actual treatment - e.g., any tests carried out by external laboratories, or references to specialists outside the hospital itself. These 'secondary' providers are health agencies in their own right, in regard to the Health Information Code and Privacy Act.

16. The Privacy Commissioner has recently published a report on Medical Records Databases which raises some serious concerns about the extent of centralised record-keeping of health care transactions for individuals in New Zealand. Most of this record-keeping, by health funding and planning agencies, appears to relate to New Zealand permanent residents, and is associated with the National Health Index (NHI) Number allocated to each individual.

17. It is not clear if temporary visitors would be allocated an NHI or if information about their treatment would be passed to the Regional Health Authority, the Health Funding Authority, and the Ministry of Health. While all these agencies are themselves subject to the Health Information Code and Privacy Act, the report suggests that the Code rules may not be fully complied with by all of the agencies involved. Disclosures to the various health agencies would almost certainly fall within the 'directly related purposes' allowed by Rule 11, but there are questions about the notification of patients in accordance with Rule 3 and the accountability requirements of the Act and Code (see below).

Data Quality and Proportionality

18. A health agency must ensure that it takes reasonable steps to ensure that health information is accurate, up to date, complete, relevant and not misleading (Rule 8). Hospitals in New Zealand have been given practical advice by the Privacy Commissioner on how to comply with this rule, such as by checking records with the patient, and ensuring that computer software checks for expected values.

19. There is also a requirement not to retain health information for longer than is required for lawful purposes (Rule 9). Public hospitals are subject to some specific retention requirements in other laws, such as the Health Act and Hospital Regulations and Medicine Regulations. Under normal circumstances, a patient's records would be kept by the hospital for 10 years, and could only be disposed of in accordance with a schedule under the Archives Act.

20. The EU Directive defines health data as one of the 'special categories' of Data (Article 8). The New Zealand Privacy Act provides no additional protection for these data.

However, the Directive itself exempts the provision and management of health care from the processing prohibition (Article 8(3)).

Security

21. Again, the source of obligations about security of health information is found in the Health Information Privacy Code. Rule 5 requires health agencies to adopt reasonable security safeguards to protect personal information against loss and unauthorised access, use modification or disclosure. They must also take reasonable steps to ensure that security is observed by anyone to whom they disclose information from the record.

22. Security has always been taken very seriously by public hospitals, and the their IT and manual record systems are subject to an elaborate range of physical and logical security measures, which have been reviewed to ensure compliance with the security principle of the Privacy Act.

Access and Rectification

23. The New Zealand Health Information Privacy Code includes the same access and correction rights (Rules 6 and 7) as the general Privacy Act, but also limits private sector health agencies from making a charge for the exercise of those rights except in specified circumstances (repeated requests and copies of x-rays, videos or CAT scans). Public sector health agencies are required under the Act to give access free of charge.

24. In this case study, the patient would be able, after his treatment, and while still in the country, to obtain access to any health records that had been created by any New Zealand health agency which had been involved in his treatment. Access under the New Zealand Code is to both facts and opinions, and the grounds for denying access are strictly limited (those in Part IV of the Privacy Act apply to the Code) and can be challenged (see below under Accountability). The patient would however lose the access right once he left the country, as section 34 of the Act limits this and the correction right to citizens, permanent residents and non-residents actually in New Zealand. The hospital may nevertheless as a matter of policy respond to requests from overseas from a former patient.

25. A right to request amendment of health information, by way of correction or addition, is provided by Rule 7, and again the general Privacy Act mechanisms for dealing with disputes about the content (Part V) apply. As with access, these rights only apply to non-residents while they are in New Zealand, although they could continue to see through any action commenced while they were in the country..

26. If they make corrections as a result of an individual's request, health agencies are required, where reasonably practical, to inform anyone to whom they have previously disclosed the information in question (Rule 7(4)).

Onward Transfer Restrictions

27. In the context of most foreseeable transborder transfers, such as those associated with the treatment of a foreign patient (e.g., consulting overseas specialists) further disclosures would be subject to the general provisions of the New Zealand law relating to disclosures, security and access discussed above. The Health Act requires health agencies to disclose relevant information to overseas heath care providers, for treatment purposes.

28. The NZ Privacy Act does not currently contain any provisions which restrict the transfer of personal data outside New Zealand. The Commissioner, in his recent review of

the Act, invited submissions as to whether such a provision was needed (partly in light of Article 25 of the EU Directive). The Commissioner is expected to issue his report on the Review in October, 1998.

29. The only provision in the New Zealand Code or Privacy Act that expressly regulates the transfer of personal health information to other jurisdictions is section 10 of the Act. It applies all of the relevant principles (5 to 11) to information held outside New Zealand by a New Zealand agency, although an additional 'exception' is granted to the non-disclosure principle for any action an agency is required to take by or under any law of an overseas jurisdiction. It is assumed that section 10 applies equally to Rules 5-11 of the Health Information Privacy Code.

30. There may, however, be some difficulties in effectively investigating or enforcing these rights in the event of an alleged breach by an interstate or overseas third party (see below under Accountability).

31. Transfer outside New Zealand might also occur for the purpose of conducting health research. The definitions of health information in the New Zealand Code excludes de-identified information. But if it was proposed to disclose (or just to use) *identifiable* information about a patient for research, this would have to be in accordance with the specific exceptions for research set out in Rules 10 and 11, or with his informed consent.

32. Rule 5 of the Code also requires health agencies when disclosing information in connection with the provision of a service to take reasonable steps to prevent unauthorised use or disclosure.

Remedies

33. The New Zealand Privacy Act provides for complaints about breaches of the Act to be made to the Privacy Commissioner. Clause 8 of the Health Information Code goes further in requiring health agencies to have a procedure for handling privacy complaints, although it is clear that individuals can go straight to the Privacy Commissioner with complaints about either breaches of the Code Rules, or of the procedures relating to requests for access or correction.

34. This right applies in most cases to any individual about whom data is held - they do not have to be New Zealand citizens or even residents, with the exception that the access and correction rights (IPPs 6 & 7) do not apply to non-residents unless they are actually in New Zealand. With this exception, a foreign national would enjoy all the rights given to individuals under the law. The Commissioner's staff can assist a foreign patient and try to conciliate or mediate the complaint. If this is unsuccessful, the Commissioner can refer the matter to a separate Proceedings Commissioner, who will in turn decide whether to take the case to the Complaints Review Tribunal. The Tribunal can make an order prohibiting a repetition of the action complained about, and/or require the interference with privacy to be put right. The Tribunal can also require the respondent agency to pay damages or compensation.

35. It should be noted that very few complaints proceed as far as the Tribunal; most are resolved at an earlier stage. Also, there is a substantial complaints handling backlog due to resource constraints, with individuals typically having to wait twelve months for investigation of their matter to even begin, unless it is assessed as urgent.

Accountability

36. The New Zealand Privacy Act (s.23)) requires health agencies to designate a member of staff as Privacy Officer, responsible for privacy and access matters, including encouraging compliance.

37. The hospital policy of client confidentiality is emphasised in routine training for employees. Security in particular is emphasised, and each employee signs a non-disclosure agreement. Misuse of personal information of patients would result in the dismissal of an employee.

38. The Privacy Commissioner has a function to enquire generally into any matter, including any law practice or procedure in the private or public sector, but has no express audit or inspection powers under the Privacy Act outside the investigation of complaints and the conducting of audits on request. The Privacy and Proceedings Commissioners, and the Complaints Review Tribunal, are independent statutory appointments at arm's length from government.

39. Aside from the Health Information Code under the Privacy Act, many health care professionals in New Zealand are subject to strict professional discipline which has statutory backing. Complaints about breaches of the NZMA Code of Ethics, and of other similar codes, can be taken up with statutory registration boards, which can impose sanctions. But apart from supporting the principles of non-disclosure and informed consent, these standards do not otherwise generally deal with other privacy issues. The Health and Disability Commissioner may be able to deal with any residual privacy complaints which fall outside the Privacy Act's jurisdiction, but within the scope of the Health and Disability Services Consumers' Rights Code**.**

Conclusions

40. For transfers of personal data into the health care system in New Zealand, the 1993 Privacy Act and 1994 Health Information Privacy Code appear to contain both the major privacy principles and accountability mechanisms equivalent to those set out in the EU Directive and member states' laws.

41. Individuals, including foreign nationals, have legal rights under the law. The Act has also created a comprehensive system of supervision and enforcement through the Privacy Commissioner, lacking only a pro-active audit role, and associated complaints review machinery, (although the complaints backlog is disturbing).

42. Personal information about Europeans receiving medical treatment in a New Zealand hospital is therefore protected by law in a way which in most respects meets the test of adequacy envisaged by the Article 29 Working Party in relation to Article 25 of the EU Directive. The only limitation on a non-resident's rights relative to a New Zealand citizen or permanent resident is that he or she cannot make an access or correction request from outside the country.

43. The absence of a comprehensive onward-transfer provision in the law would only be an issue in this case study if personal information about the patient was sent on to a third country without his consent, and this seems unlikely. The New Zealand law does provide some protection if a health agency itself holds personal data overseas, but not if it transfers the data to another person and loses control of them. This is however unlikely to be an issue in the case of medical treatment. It would therefore be appropriate to assess the legal framework as providing adequate protection *provided* there is no transfer of data offshore outside the New Zealand health agency's control.

44. However, an issue raised by this case is the extent to which the mere existence of an apparently adequate privacy or data protection law can be taken to ensure adequate privacy protection. Evidence as to whether the Privacy Act mechanisms are working satisfactorily is mixed. The Privacy Commissioner's office is active in promoting the law and handling complaints (although the complaints backlog is disturbing); cases have progressed through the mechanisms to the tribunal and courts in some cases, and remedies have been provided for breaches of the law, including the payment of compensation.

45. Most public health agencies have taken their responsibilities under the Act and Code seriously, have issued guidance for staff and have conducted training. Personal information handling practices have been reviewed and adjusted to comply with the Act and Code. Without conducting a detailed audit of a hospital it is impossible to guarantee that personal information about an overseas visitor patient will be handled in total conformity with the law, but this will always be the case with any organisation. There is no reason to suppose that it will not be, but the report on Medical Records Databases referred to above suggests that some health agencies that may receive information about patients may not be complying in all respects.

46. However, the important fact is that the hospital and other health agencies involved in any patient's treatment, and those receiving data for administration and planning purposes, are all liable under the Privacy Act for breaches of any of the Health Code rules and that comprehensive and easily accessible remedies are available to a patient if his or her privacy is breached (with the exception of the limited access and correction rights).

Medical/Epidemiological Data

(f) *United States of America*

The Nature and Circumstances of the Transfer

1. USPHARM is an American multinational pharmaceutical manufacturer with corporate activities located primarily in several northeastern states in the United States, and with operations in many other countries. The specific company activity relevant here is the testing of new drugs on patients through clinical trials.

2. Clinical trials on patients may be conducted in different countries. The company recruits independent investigators (physicians), and the investigators in turn find patients with appropriate medical conditions who are eligible and willing to participate in the clinical trial. Sometimes, a trial may be run directly by the company.

3. One or more institutional review boards or ethics committees typically approve the protocol that controls the terms and operations of a trial. They also review the informed consent agreement used in the trial. The investigators tell patients about the trial through informed consent agreements that typically explain the experimental procedure or therapy, the duration of the study, the risks, the procedures for withdrawing from the study, and how information from the study will be used and disclosed.

4. Investigators report patient information to USPHARM in a form that normally omits any overt identifiers. At its facility in the United Kingdom, USPHARM enters the information in a database that can be accessed at company locations in the United States. Data from a trial maintained in this database are typically processed in the United States and ultimately submitted to the United States Food and Drug Administration (FDA), the federal drug regulatory agency. The company may make similar submissions to drug regulatory agencies in other countries. The procedures and requirements vary from country to country. This case study focuses on the processing in the United States of patient information that originated in one or more European Union (EU) Member States and that was initially processed in the United Kingdom.

5. The EU investigators maintain fully identifiable patient data. However, patient-level information provided to USPHARM and exported through its central database to the United States normally contains no overt identifiers. Thus, a data subject's name and address will not normally be maintained in the USPHARM database. Exported data contains birth date, an identification number assigned for use in the study, and sometimes a patient's initials. On occasion, a hospital identification number appears in the records obtained by USPHARM. The company expresses some uncertainty about the applicability of the requirements of the EU Data Protection Directive to indirectly identifiable data, which it processes to satisfy other regulatory and scientific needs.

Overview of the Regulatory Environment for This Case

6. USPHARM's policy is to comply with applicable regulatory guidelines or local country requirements. The company also requires that its clinical trials comply with the World Health Organization's Declaration of Helsinki regarding recommendations guiding physicians in biomedical research involving human subjects. The Declaration of Helsinki establishes basic principles for the conduct of clinical trials involving human subjects. It recognises the importance of the privacy of the data subject, but it offers no detailed guidance on the application of fair information practices.

7. Research activities that involve human subjects and that are regulated by United States departments or agencies are subject to federal rules for the protection of human subjects. The rules address the role of institutional review boards and the requirements for informed consent. Institutional review boards must consider whether a research activity has adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data. However, the rules offer no specific guidance on privacy, confidentiality, or fair information practices in general. Otherwise, no specific federal or state statutes impose any direct fair information practice obligations on pharmaceutical manufacturers.

8. Any personally identifiable data disclosed to and maintained by federal agencies could be subject to the fair information practice rules found in the Privacy Act of 1974. This law applies to most but not all personal data maintained by federal agencies. The Act contains a complete code of fair information practices, including notice, access and correction rights, use and disclosure limits, and enforcement. However, the data normally submitted to the FDA by USPHARM would not have overt identifiers. Therefore, it is unclear that the data would qualify for protection under the Privacy Act of 1974. Even if submitted data had personal identifiers, it might not be subject to most Privacy Act requirements if the FDA did not actually retrieve the data by personal identifier. In addition, foreign nationals have no rights under the Act.

Purpose Limitation, Transparency and Opposition

Collection

9. In a clinical trial, data collection occurs in the course of a physician-patient relationship. The physician-investigator collects patient-identifiable data following the rules set out in protocol and USPHARM's instructions. From the patient's perspective, however, the collection of trial data appears no different than any other data collected by any physician from a patient. Indeed, the physician may be the regular health care provider for the trial participant.

10. A standard informed consent agreement identifying the purposes of the study must be signed by participating data subjects. The agreement obtains consent for the sharing of records with USPHARM and with drug regulatory authorities. The consent agreement also states that hospital or physician office records may also be made available to USPHARM. Data subjects are told that their records will not be made public 'to the extent permitted' by applicable laws and regulations. Data subjects are also told that they will not be identified in published studies.

11. One signature from the data subject on the informed consent agreement covers all aspects of the agreement, and no separate signature or check-mark highlights the disclosure elements. The current informed consent agreement used in the United Kingdom is being revised. According to the company, the standard informed consent agreement now used in the United States is similar to that used in the United Kingdom but not as detailed. The company reported that it expects to revise the model agreements that it uses, and hopes to use a similar standard agreement addressing fair information practices for all clinical trials in all countries. The analysis presented here reflects the informed consent agreement used in the United States. Because the terms of the disclosure that are given to EU citizens are important to the analysis and may be more specific in the United Kingdom, the discussion here may be somewhat unfavourable to the company.

Use and Disclosure for USPHARM's Purposes

12. The disclosure notice on the consent form is short, and it does not carefully spell out the details of disclosure. For example, the form does not state that USPHARM may disclose data to contractors, agents, or consultants who might process the data in the course

of the trial. The form does not acknowledge that data are maintained on a company network accessible in other countries.

13. USPHARM maintains clinical-trial data for purposes of the specific trial. It also retains the data on a long-term basis for possible use in related or unrelated research. The original clinical-trial data may be useful in the future if questions arise about safety or efficacy of the drug originally tested. The records may also be used in other, unrelated types of research to test new hypotheses or explore new scientific or medical insights. The brief statement of purpose in the consent form does not address the long-term retention of data or the possibility of their use in other research activities. Thus, under current practice, a patient would receive no general or specific notice of possible new data uses. USPHARM is currently reviewing its policy and its notice about disclosure. The company plans to offer a more complete notice about disclosure practices. Other parts of the standard consent form affecting fair information practices are also being revised.

14. USPHARM offers no public notice of its clinical-trial information policies. Each participant receives at least some personal notice of information practices from the investigator as part of the informed-consent process. Each participant must consent before the investigator collects and reports any personal information. A data subject can revoke consent and withdraw from the trial at any time.

Disclosure to Third Parties For Other Purposes

15. Patient data may be obtained by government agencies in the United States in a variety of ways. The company collects and processes clinical-trial data for submission to the FDA. The FDA must approve a drug before it can be marketed, and the agency requires detailed trial data in order to make a decision. The type of patient identifiers submitted to the FDA is discussed below. It is also possible that similar information will be submitted to state pharmaceutical regulators, but this type of disclosure is said to be rare. In addition to the routine submission of patient-level data to the FDA, it is also possible that the FDA would from time to time require more detailed and identifiable data as part of its oversight and monitoring of the clinical trial process. For example, the FDA might want to determine that the underlying data actually existed and were not created by an unscrupulous investigator. USPHARM also monitors its investigators for the same purpose. In either case, USPHARM would retrieve or review the underlying data held by the physician-investigator for use in a company or FDA audit.

16. Other federal government agencies, such as the Centers for Disease Control, the National Institutes of Health, or the Veterans Administration, might co-operate in a clinical trial. Some state agencies, such as state-operated university health programmes, might also co-operate in a trial. Some sharing of data with these agencies could occur during the course of a trial.

17. Disclosures to law-enforcement agencies are another possibility. In theory, a variety of law-enforcement activities could generate requests or subpoenas for information. However, demands by law enforcement agencies (other than the FDA) are rare. Data might also be sought for use in private litigation. USPHARM's policy is to resist all such disclosures, whether by subpoena or otherwise. The company will fight these disclosures without the consent of the data subject. The company assesses each case that arises on its own merits.

Data Quality and Proportionality

18. USPHARM imports data into the United States for ultimate submission to the FDA. Published FDA rules instruct companies not to include the names and addresses of individual patients. Records must be coded, and the codes retained by the investigator. The

company must, however, retain the ability to identify individual patients in case of an FDA investigation.

19. USPHARM has a high level of concern about the quality and accuracy of its data. The company has a policy about data quality, and it enforces it through software controls and internal practices. In addition, the FDA has rules requiring accurate information. If an investigator in the United Kingdom corrects a record, and the change is recorded in the company's central database, the corrected record will thereby be accessible in the United States.

Security

20. USPHARM has rules, policies, and technical measures designed to protect the security of its data and databases. The company maintains a considerable volume of confidential corporate information as well as patient information, and it has a significant incentive to protect it. The company does not classify data into different levels of sensitivity for purposes of security.

21. The company has a written security policy, but it does not pointedly inform its employees about it. Security is enforced through computer controls such as passwords, access controls that keep employees from seeing data unnecessarily, and audit trails. Encryption is used for external transmissions but not for internal storage.

22. USPHARM does not have a dedicated security officer, but it does conduct internal audits that address security requirements.

Access and Rectification

23. USPHARM does not consider patient data available in the United States to be identifiable. As a result, it has no procedures to provide for access to data by the data subject. Any records available in the United States are also available in the United Kingdom, and access through the United Kingdom data protection law is presumably available. In addition, the fuller and more clearly identifiable records maintained by the investigator would also be available for access and correction by data subjects much like any other health-care records.

24. The company reports that it has not received any requests in the United States for access to or correction of patient records received from abroad. The only exceptions may result from discovery requests connected with litigation against the company.

Onward Transfer Restrictions

25. Data transferred by USPHARM from the United Kingdom to the United States for drug regulatory purposes may also be transferred to other countries for similar purposes. Because the data originate in the same database, it can be difficult to describe meaningfully whether the data exported to the United States are 're-exported' to another country or are directly exported again from the United Kingdom to the third country. Technical details of the transfer may affect the characterisation of the transfer as an export or re-export. Regardless of the technical details, the data originating in the United Kingdom can be shared with company offices in several other countries.

26. USPHARM does share data with data processors (contract research organisations) who assist the company in analysing and preparing the data for submission to FDA. Standard contracts with independent data processors impose requirements to safeguard proprietary data. However, these contracts contain few details and do not expressly address

fair information practice requirements. The company maintains oversight of its contractors through audits and inspections to ensure compliance with requirements. The company is formalising a policy on fair information practice requirements for company contractors.

Remedies

27. The informed consent agreement signed by trial participants includes the name and telephone number of a person to contact to answer questions. However, the form does not identify any formal complaint mechanism. A data subject could presumably complain directly to the investigator. A data subject could also complain to the FDA, although it is unclear if the agency would have any interest in investigating fair information practice violations. An aggrieved data subject could also seek to file a lawsuit over breaches of fair information principles. However, no specific federal or state statutes impose any direct fair information practice obligations on pharmaceutical manufacturers. Relief might be available for breach of contract or for tortious conduct, but the success of any such lawsuits is uncertain. Precedents for this type of litigation are not apparent.

28. Because there are no readily identifiable remedies, it is difficult to assess whether remedies available to foreign nationals would be equal to those available to United States' citizens. The federal Privacy Act of 1974 does not grant any rights to non-resident foreigners, so that Act's remedies against the FDA would not be available even if the Act applied to clinical-trial records submitted to the agency. No other relevant federal or state statutes with limitations on relief for non-resident foreigners have been identified. Contract or tort remedies, if available at all, would likely be available equally to all.

Accountability

29. USPHARM has some policies and practices advising its employees about the proprietary nature and sensitivity of the information that it routinely maintains. However, no systematic policy documents focus expressly on privacy maters. The company does not have an identifiable privacy official. No training in privacy or fair information practices is offered to company employees.

30. The company does not have an internal mechanism for approving proposed new uses or disclosures of personal data. Thus, no policy or mechanism regulates the use of data retained by USPHARM after the conclusion of a clinical trial. However, company activities are regularly controlled through the development of protocols approved by institutional review boards, and these boards may impose limitations on new uses of data. In addition, the company has a culture that recognises the confidential nature of patient data. The company also employs many health professionals subject to professional secrecy obligations.

31. Routine oversight of clinical trials by the FDA does offer the prospect of some external review of company data and company practices. However, the FDA has not traditionally focused on fair information practice concerns other than data quality. The requirement to submit data to the FDA does provide an incentive for the company to review its data files to make sure that rules have been followed. However, the FDA's limited interest in the full range of fair information practices suggests that the incentive offers few actual protections for data subjects.

Conclusions

32. A principal difficulty in assessing the adequacy of transfers by USPHARM to the United States is the uncertainty over the applicability of privacy rules to the semi-identifiable data that are most routinely transferred. If the data were considered identifiable,

then the company would be expected under data protection rules to offer access and correction rights to patients. However, in order to provide those rights, the company would have to include overt identifiers in the transferred data. This leads to the somewhat perverse result that more identifiable data must be exported in order to enforce fair information practices. Arguably, the data may be better protected against misuse and improper disclosure in its current semi-identifiable form.

33. Many problems with the export of clinical-trial data would disappear if data were exported in a completely anonymised form. However, clinical-trial oversight requires the potential for audit and identification of records. The justification for maintaining the possibility of identification cannot be easily dismissed.

34. It is not necessarily a simple matter to decide when information is completely anonymous. The conclusion depends on what other information is available to assist in the identification of individuals and on how much effort someone would expend to make the identification. With increasing computerisation of data from diverse sources including public registers and commercial activities, the ability to identify records is greater than in years past. The same computers make the technical task of sifting and matching data simpler as well. No single principle or policy can assure that any given set of data is anonymous. No sharp lines of demarcation are found on the continuum between completely anonymous and completely identifiable. Current practices of USPHARM that rely on initials and birth date together with a project-specific identification number create records that may not be especially difficult to identify in some instances if someone were inclined to try. However, identification of the clinical-trial data exported to the United States would not be simple, and is difficult to imagine circumstances that would warrant the significant effort that would be required.

35. Better forms of coding or anonymising data exported from EU Member States will lessen the possibility of identification. Encryption, aggregation, and micro-aggregation may be useful in allowing sufficient use of data for regulatory and other purposes while lessening the risks of identification. Legal or contractual prohibitions against the 'reverse engineering' of anonymized data might also increase both the likelihood that data will remain anonymous and the prospect that those who seek to add identifiers to anonymous data will be punished. For clinical trials, it will likely take international co-operation among pharmaceutical companies, drug regulators, and data protection officials in order to develop the right set of technical, legal, and contractual rules that will allow maximum use of data with a minimum risk to the confidentiality interest of clinical-trial participants.

36. For most fair information practice requirements, USPHARM does not currently appear to have sufficiently specific rules or policies to meet generally accepted fair information requirements. Security may be the only area where company policies appear to be adequate. In other areas, including transparency, purpose limitation, and accountability, current USPHARM policies are too vague or unfocused.

37. USPHARM knows about the requirements of the EU Data Protection Directive and of the impending deadline. The company expects to address the deficiencies and gaps in its current policies and practices. In addition, USPHARM and other pharmaceutical companies working through industry trade associations are co-operating to standardise clinical-trial information practices through the development of a code of conduct for the pharmaceutical industry. The code of conduct has been discussed informally with EU data protection authorities and with other regulatory authorities. It appears that a considerable effort is underway at several levels to adopt more express fair information practices for clinical trials and related activities. Nothing in the company's current policies is expressly inconsistent with fair information practices, but much supporting detail is missing, procedures are not defined, and notable gaps exist in those policies.

38. Scattered state and federal laws offer limited and incomplete privacy protection to some health-care records maintained in the United States. However, these laws are not

likely to afford any relief to clinical-trial participants. While the records of some American-based physician-investigators may be covered by these laws, records transferred to USPHARM from overseas are not likely to be subject to any statutory privacy rules while in the hands of USPHARM. In any event, the disclosure to USPHARM is authorised by data subjects' consent, although the consent might not be detailed enough to provide sufficient notice of all other actual and potential disclosures. Because of the lack of applicable American privacy laws, the company itself remains the only source of fair information practice standards at present.

39. Overall, it is difficult at present to point to any codes, laws, or systems that ensure a good level of compliance with fair information practices. The company itself is the only real source of standards, and current company policies are significantly incomplete. Support for data subjects is also totally dependent on the company, and the company has taken no steps to provide assistance to them. It is also hard to point to existing remedies that are likely to afford relief to aggrieved data subjects. The result is that many gaps in data protection exist for clinical-trial data exported to the United States. The uncertainty of the status of the data, because of its absence of overt identifiers, is a significant factor.

Conclusions about Medical/Epidemiological Data

1. The five cases which are based on the scenario of the transfer of individual patient records from a European Union country to hospitals in third countries demonstrate a number of uses to which medical treatment records might be put. In each country, health care provision can also encompass many associated activities that can occur within a number of public and private organisations, besides the primary health-care provider.

2. Only comprehensive data protection standards can provide that 'seamless protection' for health care records when they are used by other institutions such as insurance companies, employers, researchers, medical informatics businesses, etc. Adequate protection for all primary and secondary uses of personal health information is, therefore, greatly dependent on whether the jurisdiction has a comprehensive data protection law. In Hong Kong and in New Zealand, public and private-sector data protection laws generally oblige all institutions that might conceivably receive personal health information to abide by basic fair information principles. A similar law exists in the Canadian province of Quebec.

3. In Canada, Australia and Japan, there is a patchwork. In the Australian and Canadian cases, two relatively progressive health information statutes recently passed at sub-national levels were analysed. Both appear generally consistent with the EU Directive, so long as the records are held by institutions covered by the respective laws. In other sub-jurisdictions in these three countries, there is likely to be a less rosy picture. In none of these countries does the data protection law follow the record, leading to the perverse result that data subjects might have rights over their health information when it is held by a public hospital, but not when it is retained in the office of a private doctor. In both Canada and Australia, efforts are underway to remedy the patchwork problem at provincial and state levels, respectively. There are few such initiatives in Japan.

4. Health-privacy legislation is also supplemented by common-law duties of confidence applying to physician/patient relations, and of course the Hippocratic oath. But these long-standing ethical precepts do not address all elements of fair information practices. Codes of practice also perform an important role, although these vary considerably in their coverage and enforceability. The Code of Practice for Health Information in New Zealand, for example, is a comprehensive code, issued under the Privacy Act with the force of law, and overseen by the Privacy Commissioner. The recently issued Canadian Medical Association’s Health Information Privacy currently embodies no enforcement mechanism or sanctions. This comparison indicates that the term 'privacy code of practice' can embrace a range of different self-regulatory instruments.

5. The observation of meaningful remedies, assistance to data subjects and mechanisms for accountability is also tied to the presence of a general data protection law. In other jurisdictions, there may be relatively powerful supervisory authorities that nevertheless have no jurisdiction over some users of health-care information. This is particularly apparent in Canada and Australia.

6. The United States case deals with a very different scenario concerning the transfer of data within a multinational pharmaceutical company for clinical trials. This was the only jurisdiction in which a realistic case study on clinical trials could be researched. Nevertheless, the conclusions about the overall adequacy of protection mirror those in the other countries which lack comprehensive data protection legislation. While the medical transfer to the United States was limited to clinical data, it is widely acknowledged in the United States that overall protections for health-care records offer a patchwork of incomplete privacy protections for patients in most contexts. Consequently the adequacy of protection for clinical trial records is heavily dependent on the practices of the company concerned, and particularly on the transfer of personal data in semi-identifiable form. The case questions the applicability of fair information practices to data that can only be re-identified under extraordinary circumstances or with considerable effort.

Data in Electronic Commerce

(a) *Australia*

The Nature and Circumstances of the Transfer

1. BONZA is an Australian-owned retailer and mail-order company that has been in existence for 13 years, based in outer Sydney, New South Wales. Originally just a magazine publisher, founded in 1986 with the mission of showing Australia in a positive light, BONZA soon branched out into a range of other products and services, including merchandise sold through a catalogue, and from 1991, a chain of physical shops. As a membership organisation, BONZA also sponsors scientific research, environmental and community projects and expeditions. It has developed a familiar brand name image and thus a loyal customer base around the world.

2. Although BONZA has 30 shops, it has always done most of its business through mail-order catalogue sales and an increasing volume of business is being done through its Internet World Wide Web site. The Web 'shop' offers more than 250 products, and it is also possible to join the society and subscribe to the magazine (the two go together) on-line.

3. The site uses one of the proprietary Internet shopping products - NetCommerce™ - which allows browsers to accumulate orders in a 'shopping trolley' which they eventually take through a check-out, completing details for both billing and shipping, and with a range of payment options including giving credit card details through an encrypted link, or using e-cash from a system established by one of the Australian banks.

4. European customers using the Internet to access BONZA's website and order merchandise will of course be transferring data about themselves to BONZA in Australia, via their own and BONZA's service providers and an unknown number of intermediate carriers and servers.

5. The European Union (EU)'s Data Protection Working Party has taken a provisional view that in putting a website on the World Wide Web, 'publishers' are 'processing' personal data on the computer equipment of the person browsing, and/or on file servers located in the browser's home country. It follows that any web publisher anywhere in the world is technically a data controller subject to the data protection law of any and all countries in which people access their site. This interpretation gives rise to some difficulties in terms of reasonable expectations of awareness of obligations, let alone compliance and enforcement. For the purposes of this case study, the liability of BONZA under European data protection laws will not be considered further. The case study will concentrate on other privacy protection that may apply to data about European 'browsers' accessing BONZA's website.

6. This assessment necessarily involves looking at protection for personal information held both by BONZA and by other intermediaries such as BONZA's Internet service provider and other parties involved in the transmission of data between BONZA and a European Internet customer.

Overview of the Regulatory Environment for This Case

7. There is currently no privacy law in any Australian jurisdiction that applies to the activities of a mail-order retailer such as BONZA, unless they decide to offer credit terms (defined as payment deferred by seven days or more), in which case they would be subject to enforceable credit information rules under the Commonwealth Privacy Act 1988. Accepting credit-card payments does not bring a retailer under these rules as it is the credit-card issuer that is the 'credit provider' under the Act.

8. Telecommunications carriers, carriage service providers, and content providers are subject to varying degrees to the Telecommunications Act 1997, which includes strict use and disclosure limitations in Part 13 (subject to statutory exceptions in Parts 13 to 15). There is also an elaborate process whereby they will, again to varying degrees, be subject to a number of codes of practice, including one expressly on the privacy of customer personal information. These codes are being developed by a self-regulatory body, the Australian Communications Industry Forum (ACIF), through a consultative process, but will ultimately be registered with the Australian Communications Authority (ACA), thereby acquiring a measure of statutory force. Repeated breaches of a code of practice can lead to sanctions, including, ultimately, revocation of a licence to provide carriage services.

9. Internet access providers (organisations which host websites or provide connection to the Internet) are considered carriage service providers under the Act, and are subject to the full range of regulation, including the Part 13 confidentiality provisions, the privacy and other codes of practice (once in effect), and the Telecommunications Industry Ombudsman (TIO) scheme for complaints and dispute resolution. However, content service providers (the category into which BONZA falls) are much more lightly regulated, and it is still unclear how they will be affected by the new Telecommunications co-regulatory regime.

10. There are moves towards codes of practice both for direct marketers (through the Australian Direct Marketing Association (ADMA)), and for those involved in the Internet industry, including content providers, through the Internet Industry Association (IIA). These codes are referred to where applicable in this case study. Both ADMA and IIA have declared their intention to revise their draft codes to incorporate the Privacy Commissioner's National Principles for the Fair Handling of Personal Information. This is a set of privacy principles put forward by the Commissioner in February 1998 following intensive consultation with business, government and consumer representatives. They have been drafted with the EU Directive very much in mind and are regarded by the Commissioner as being close to international ‘best practice’, although they are still being finalised. The Victorian government has also said that it will adopt the Commissioner's Principles as the basis for a statutory regime to be introduced into Parliament later in 1998.

11. The regulatory environment is further complicated by the proposal to register the IIA Code not under the Telecommunications Act but under the Broadcasting Services Act. This will invoke a supervisory regime involving the Australian Broadcasting Authority (ABA). Legislative amendments will be required to provide for this proposal, and the details are as yet unclear.

12. BONZA is not currently a member of either ADMA or the IIA, although it is eligible to join either or both. BONZA's Internet service provider, WEBFINE, is a member of the IIA, and both WEBFINE, and all the carriers (telcos) used by BONZA and WEBFINE are subject to the Telecommunications Act regime.

13. The banks which receive information in the course of approving payment for goods ordered from BONZA's Internet site, whether by e-cash, credit card or cheque, are not currently subject to any specific privacy law in relation to that information, although they have a common-law duty of confidence which is taken very seriously by Australian banks and is reflected in the Banking Code of Practice. This Code is subject to a voluntary, self-regulatory Banking Industry Ombudsman (BIO) scheme for complaint and dispute resolution. The Australian Bankers Association (ABA) participated in the development of the Privacy Commissioner's National Principles, and banks are currently considering whether to adopt those principles in their self-regulatory framework, and if so, how.

Purpose Limitation, Transparency and Opposition

Collection

14. A customer shopping online with BONZA is prompted to provide a name, e-mail and postal address, phone and fax numbers, membership number (if applicable) and any special instructions. The screen form asks separately for billing and shipping details. There is an option for repeat customers to store these details so that they do not have to fill them in each time. Choosing this option brings up screen which does have some information about personal information use.

15. When the customer has completed at least the main personal details (name, billing postal address and e-mail address are mandatory), they proceed to payment options. An order number is presented, and there is a choice of e-cash (for which users have to have opened an e-cash 'wallet' with a particular bank), credit-card payment either on-line, by phone or by fax (an order form is e-mailed), or by mail (goods are not shipped until payment has been received). There is no specific message about security or encryption accompanying the payment choice menu; there is only an item about secure transactions in the BONZA members' newsletter, which is not easy to find.

16. The BONZA website sets a cookie on users' computers by default. If the user has configured the browser to warn of cookie requests, then (in Internet Explorer v4) a standard Microsoft prompt appears asking for permission to set the cookie so as to 'provide a more personalised browsing experience' and warns that the screen may not display correctly if the request is turned down. In practice, it seems to be possible to proceed through the shopping and ordering sequence without enabling cookies, although this does require rejection of the request after every interaction.

17. By contrast, if the user chooses the e-cash payment option, the bank page he or she is taken to has a very prominent link to the bank's cookie policy, which gives a very full and clear explanation of the function and personal information implications, including options relating to per-session enabling of cookies. It is unlikely, but not impossible, that a European customer would go to the trouble of opening an Australian e-cash account, although this will become more likely when internationally accepted e-cash accounts are offered.

18. There is no general data protection law in Australia that governs the collection of personal information in the private sector. Retailers and publishers, like all other businesses, are subject to the Commonwealth Trade Practices Act, and to State Fair Trading laws, and these contain provisions prohibiting unfair or unconscionable conduct, such as misleading advertising and high-pressure sales techniques. Although it would arguably be possible to bring a case under this consumer protection legislation about unfair data collection, there are no known precedents.

19. As mentioned above, BONZA is not a member of the IIA. The draft IIA Code has as one of its aims 'to provide standards of confidentiality and privacy afforded to users of the Internet', and a principle that 'the privacy of users' details obtained by Code Subscribers in the course of business will be respected.' As well as a section specifically on confidentiality and security (see below), it also says the following:

'Code Subscribers will collect details relating to a user only:

(a) if these are relevant and necessary for the provision of the service or product that the Code Subscriber is engaged to provide; or
(b) for other legitimate purposes made known to the user prior to the time the details are collected.' (Clause 9.1)

It also says:

'In this part of the Code, references to the collection of details include collection of details by active request or inquiry and collection of details by passive recording of actions or activity.' (Clause 9.4)

20. Further guidance on the collection of information via cookies is given in consumer protection principles for electronic commerce issued by the National Advisory Council on Consumer Affairs in May 1998. These principles include:

'Sellers should adopt the following practices in relation to "cookies":

(a) sellers should clearly offer consumers the alternative of rejecting them;
(b) where the technology allows, there should be an opt-in basis; and
(c) sellers should not assume consumers have their web browsers set to notify them that they are about to receive a cookie.'

21. BONZA is clearly not currently meeting this standard, which is entirely voluntary. The bank providing the e-commerce facility appears to respect the principle by clearly drawing users attention to their cookie policy on their 'entry' page, and providing options if the user wishes to pursue the issue. However, one commentator has suggested that users who have simply adopted the 'default' setting of their browser to accept cookies without prompting may be taken to have authorised the collection and transmission of data.

22. BONZA is also not currently notifying people who become customers of its more general data collection practices when they purchase or subscribe on-line.

Use and disclosure by BONZA and others in connection with the transaction

23. As there is no general data protection law in Australia that governs use and disclosure of personal information in the private sector, BONZA's company policy on the use of personal data is wholly driven by its own commercial judgement and perceptions of consumer needs. The company currently collects only enough information to fulfil the orders submitted and process payment. There is no obvious 'extra' information requested that might suggest a deliberate strategy of building customer profiles, beyond what can be inferred from transaction history. However, as noted above there is no statement available on or via the website describing the purpose of collection or the proposed uses and disclosures.

24. A mentioned above, BONZA is not a member of ADMA, which currently promotes voluntary Standards of Practice for direct marketing that include a commitment to 'respect individual privacy'. The Standards include some provisions which overlap with privacy principles, including limitations on telemarketing hours, transparency about the identity of the advertiser, and a commitment to flag or remove from lists those consumers who ask for their names to be deleted, and to identify the source of a prospect's details. ADMA itself maintains preference lists which consumers can join if they do not wish to receive unsolicited offers by mail or telephone, but these are not widely advertised or well known. At present, there is no formal machinery for handling complaints or monitoring compliance with the Standards of Practice, which are entirely voluntary. ADMA has publicly announced that it proposes to incorporate the Privacy Commissioner's National Privacy Principles into a new Code of Practice, which will be launched later in 1998.

25. The IIA's proposed Code of Practice contains a section specifically on use of personal information:

'Code Subscribers will use details relating to a user only for:

(a) the Code Subscriber's own marketing, billing and other purposes necessary for the provision of the service, or
(b) purposes made known to the user prior to the time the details are collected, or
(c) other purposes with the prior consent of the user.' (Clause 9.2)

But again, BONZA is not a member of the IIA.

Disclosure to third parties for their own purposes

26. It is difficult to foresee the circumstances under which data held by most mail order businesses such as BONZA would be requested by government agencies, but there is currently no legal framework to govern their response. They would be free to disclose customer information at will, although also at liberty to decline to disclose other than in response to a legally authorised request, such as a subpoena or warrant. There are clearly some mail-order businesses, such as those supplying adult materials, or pharmaceuticals, where there are additional sensitivities and where the authorities may take an interest in activity that may be at the margins of the law.

27. A parliamentary enquiry earlier this year into Internet Commerce took evidence from the revenue-collection agencies - the Tax Office and Customs - about the risk of loss to the public revenue of Internet transactions which would attract tax or duty if conducted in more traditional ways. At this stage, there is no suggestion that additional powers are needed, and the revenue authorities already have statutory powers to obtain information in the course of investigations and pro-active audit programmes. These powers would override disclosure limitations in any likely privacy law, although those limits would probably constrain the range of informal requests for personal information which are currently made, successfully, by both revenue and law enforcement agencies.

28. The IIA's proposed Code of Practice says:

'Code Subscribers will...(c) not sell or exchange the business records or personal details of a user other than to another Code Subscriber as part of the sale of the Code Subscriber's business as a going concern.' (Clause 8.1)

'Clause 8.1 does not prevent disclosure of information with the express or implied consent of the user or as required by law. Nothing in this Code in any way releases a Code Subscriber from more onerous secrecy obligations imposed by statute or contract or equity, or other industry code of practice to which they may be bound.' (Clause 8.2)

Data Quality and Proportionality

29. There are currently no externally imposed limits for the accuracy, relevance, timeliness and completeness of personal data held by private sector organisations in New South Wales, or anywhere else in Australia.

30. The ADMA Standards of Practice contain some provisions aimed at ensuring that lists are of high quality, but these are directed at the interests of the list owners and users, and only incidentally benefit consumers.

31. The IIA's proposed Code of Practice says:

'Code Subscribers will take reasonable steps, having regard to the nature of the information, to ensure that information collected in relation to a user:

(a) to the extent that it comprises business records or personal details, can be checked by a user;
(b) is accurate, and if necessary, kept up to date;
(c) if inaccurate, is erased or rectified.'(Clause 9.3)

32. There are no externally imposed disposal requirements or time limits for retention, either in law or in the existing codes.

Security

33. Similarly, any security requirements are imposed by internal company policy rather than by law or by any currently operative industry codes of practice.

34. ADMA's specific Standards for Computerised Databases and Mailing lists contain a general list-security provision, recommending the 'seeding' of lists with dummy names as a deterrent against unauthorised mailing. The proposed IIA Code of Practice says:

'Code Subscribers will:

(a) keep confidential the business records and personal details relating to each user and will respect the privacy of users' personal communications;
(b) take adequate steps to ensure the confidentiality of business records and personal details;...
(d) refrain from intentionally examining or tampering with a user's private content without the express prior consent of the user.' (Clause 8.1)

35. BONZA emphasises on its website the security of its system. A notice on one of the more obscure lower level home pages says that 'buyers can stock their shopping baskets content in the knowledge that their transaction are secure. The encrypted system ensures that only our subscriptions department has access to this information for processing orders.' The supplier of the NetCommerce™ internet shopping software used by BONZA also emphasises security, noting on its website that it supports Secure Sockets Layer (SSL) and uses 128 bit encryption.

36. Unauthorised access to customer information on a computer, whether it were BONZA's own computer or a server belonging to its internet service provider WEBFINE, would be an offence both under the Commonwealth Crimes Act 1914 (s.76D) and equivalent State laws (e.g. the Victorian Summary Offences Act 1966 (s.9A)). The Commonwealth Telecommunications (Interception) Act 1979 provides further protection by making it an offence to intercept 'real time' communications, but is understood not to apply to 'stored' communications, even if they are only stored temporarily as part of a transmission system.

Access and Rectification

37. No law or code of practice currently obliges BONZA to give individuals access to the personal information it holds on them. Both the ADMA Standards of Practice and the draft IIA Code are silent on access, although both are due to be revised to incorporate the Privacy Commissioner's National Principles, which include access and correction rights.

Onward Transfer Restrictions

38. BONZA currently offers no guarantees about ensuring privacy protection if and when customer personal information is disclosed to third parties, whether in Australia or

overseas, although it is not obvious why they should ever need to transfer overseas. The current ADMA Standards and draft IIA Code deal with this issue only indirectly through the general security provisions (see above), but if they adopt the Privacy Commissioner's National Principles they will contain an express 'Transborder Data Flow' restriction, modelled on that in the EU Directive. It is expected that this principle will be modified to apply to onward transfers within Australia as well as overseas, to reflect the patchwork of privacy regulation between different sub-national jurisdictions.

Remedies

39. There are currently no remedies available to BONZA customers dissatisfied with the company's handling of personal information, either under law or under any codes of practice, unless the complaint included general 'fair trading' grounds.

40. If the ADMA or IIA Codes are implemented with an effective complaints-handling mechanism, and BONZA chooses to subscribe to one or both, then customers would acquire some remedies, albeit not legally enforceable ones.

Accountability

41. BONZA, and other merchants providing good and services over the Internet, are not currently subject to any external accountability mechanisms in relation to their general handling of most personal information, except insofar as State and Federal consumer protection legislation and codes provide remedies for any 'unfair' dealings. If they offer credit they are subject to Part IIIA of the federal Privacy Act 1988 and the jurisdiction of the Privacy Commissioner in relation to the handling of credit information.

42. If Victoria goes ahead with its declared intention of enacting the Privacy Commissioner's National Principles for the Fair Handling of Personal Information before the end of 1998, there will be a full range of complaints-handling, monitoring and enforcement mechanisms applying to merchants or Internet service providers located in the State of Victoria. The issue of whether this law, like overseas data protection laws, will also apply to merchants or service providers outside the jurisdiction because of their use of local processors in their transactions remains to be resolved.

43. The draft IIA Code of Practice proposes to establish a Code Administrative Council to supervise and monitor the code, and a 'code compliance symbol' which those committing to observe the Code would be permitted to display. It is proposed that complaints about breaches of the Code would initially be handled by the respondent (the organisation complained about), but with the fallback, at the complainant's request, of independent mediation, the mediator to be appointed by the chairperson of the Administrative Council. However, the costs of mediation would be shared equally, and there is no provision in the draft Code for the mediator to direct changes of practice, award compensation or impose sanctions in relation to a specific complaint. The Administrative Council would be able to issue a notice with some of these effects, with the ultimate sanction of de-registering a Code Subscriber, preventing them from claiming to comply and from using the code compliance symbol.

44. Under the ADMA proposal, there will be a new Code Authority, with an independent chair, to supervise compliance and handle complaints, with the power to impose sanctions or expel members from the Association. Details are not yet available, although it is proposed to launch the Code later in 1998.

Conclusions

45. Whether on-line or off-line, the handling of personal information collected at the time of purchase of goods or services is not a regulated activity in Australia, except in relation to credit information (subject to the federal Privacy Act), and in the telecommunications sector where a complex co-regulatory regime is being introduced. Elsewhere, information can be collected, processed, profiled, matched and used for a range of purposes, including marketing, without the prior knowledge or consent of the consumer.

46. There is legal protection against unauthorised access to information held on computers, in both State and federal 'computer trespass' laws.

47. Businesses that are members of ADMA are expected to follow Standards of Practice which incorporate some privacy principles, although there are no well-developed compliance or complaint mechanisms. Before long, members of both ADMA and the IIA are likely to be required to observe new codes of practice which should incorporate the Privacy Commissioner's National Principles for the Fair Handling of Personal Information.

48. Both codes will also have self-regulatory complaint mechanisms, although the IIA mechanism relies on shared cost mediation which could in reality make remedies for minor privacy breaches inaccessible. The Codes seem likely to rely on the traditional self-regulatory approach of expecting transgressors to make amends voluntarily, with limited options for enforcing compliance on recalcitrant members, and no pro-active monitoring or inspection function. Membership of both associations, and codes, is entirely voluntary and neither one has anything approaching total coverage of businesses operating in the direct marketing or Internet industries respectively.

49. The Victorian government's June 1998 announcement of data protection legislation to apply to the private sector should lead to at least those merchants offering Internet sales from (and possibly through) that State being subject to a binding statutory privacy protection scheme before the end of 1998. It remains to be seen if any of the other States follow suit and if the Commonwealth government moves to ensure national consistency.

50. At the moment, there are no binding or readily available voluntary rules applying to the operations of Internet merchants such as BONZA. Individuals choosing to do business with such merchants have no remedies available to them if their privacy is breached, and they have none of the rights which would be expected under any set of privacy or data protection principles.

Data in Electronic Commerce

(b) *Canada*

The Nature and Circumstances of the Transfer

1. OH! CANADA is a Canadian owned mail order company headquartered in British Columbia that has been in existence for about 40 years. Originally just a magazine publisher, OH! CANADA now promotes a large range of Canadian-made products and services. It has developed a familiar brand-name image and thus a loyal customer base around the world.

2. Its magazine business has around 250,000 subscribers internationally. Because many people in Canada buy subscriptions for friends and relatives around the world, OH! CANADA has more subscribers than actual customers (around 140,000). Approximately one-third of its subscribers live outside North America. Around one-quarter live in countries of the European Union (EU). Based on current (1997) subscription data, OH! CANADA holds personal information on roughly 54,000 European citizens, of which 37,000 reside in the United Kingdom. OH! CANADA also has a catalogue business, promoting books, videos and Canadian produced goods and souvenirs. It has around 40,000 catalogue customers, of which around a quarter live in Europe. Around 30 percent of these catalogue customers also subscribe to the magazine.

3. OH! CANADA relies to an increasing extent on direct-to-home marketing to promote its various products; there are now very few retail outlets. Most customers order subscriptions and goods by mail, fax or by a toll-free 1-800 number (only available in North America). OH! CANADA also receives requests for information from potential tourists, although these inquiries are normally forwarded to the appropriate government tourist offices.

4. OH! CANADA developed a website in 1996. This is based on a server run by the major telecommunications carrier, BC Tel. Through the website, individuals can subscribe to the magazine, and will be billed later. Online purchases can, however, be made for some of the catalogue items, by clicking on the product in question and providing name, address, phone number, e-mail address and credit-card billing information. The amount of business currently conducted online is a very small proportion of the company's total sales. Nevertheless, they see the potential for Internet marketing, especially for customers outside North America. EU customers using the Internet to access their website and order merchandise will, of course, be transferring data about themselves to OH! CANADA in Canada, via their own and OH! CANADA's service providers and an unknown number of intermediate carriers and servers.

5. OH! CANADA has been chosen for this case study because it does hold a significant amount of identifiable data on EU citizens, and because it rents its own lists, and rents lists from others through the process described below. It is probably a very representative Canadian mail-order company. Its use of electronic commerce, whilst in a fledgling stage, is also typical of the way that the Internet is currently being used to promote goods and services. Along with musical recordings, tickets, computer items and books, magazine subscriptions are currently one of the five most developed areas for electronic commerce in Canada.

6. OH! CANADA is a member of the local Better Business Bureau and of a variety of international and regional magazine publishing associations and chambers of commerce. It is not, however, a member of the Canadian Direct Marketing Association (CDMA), the principal trade association for direct marketers in Canada.

Overview of the Regulatory Environment for This Case

7. There is no general data protection law in British Columbia that governs the collection, use and disclosure of personal information in the private sector. British Columbia's Freedom of Information and Protection of Privacy Act extends to government ministries, municipalities, schools, hospitals and universities, and to the organisations of certain self-governing professions. It does not extend to companies such as OH! CANADA, nor to any other business operating in British Columbia, unless that business processes personal data under contract with a government agency. Prospective federal legislation will only cover the federally regulated private sector in the areas of banking, telecommunications, and transportation. Bill C-54 will regulate companies like OH! CANADA to the extent that it applies to personal information that an organisation collects, uses or discloses interprovincially or internationally. Customer lists that are traded as part of the list-rental process (described below) will fall under these new federal data protection rules, although the exact drawing of jurisdictional responsibilities needs further clarification.

8. Some Internet access providers (especially those affiliated with established telecommunication companies) are considered carriage service providers and will be regulated under the Telecommunications Act, which gives certain powers to the Canadian Radio-Television and Telecommunications Commission (CRTC) to 'respond to the economic and social requirements of users of telecommunications services, including the protection of privacy of individuals.' (Bill C-62, Telecommunications Act, s.7(h). Consumers could, therefore, complain to the CRTC if a privacy breach occurred by a service provider.

9. Several codes of practice guide company behaviour in electronic commerce. The CDMA claims to represent around 70 percent of the direct-marketing activity in Canada, although OH! CANADA is not a member. Members of the CDMA are required to abide by a Privacy Code designed to: give consumers control of how information about them is used; provide consumers with the right of access to information; enable consumers to reduce the amount of mail they receive, through a 'Do Not Mail, Do Not Call' service; control the use of information by third parties; ensure that companies safely store information about consumers; and ensure that they respect confidential information.

10. The Code also establishes a complaints-resolution process and the ultimate sanction of dismissal from the CDMA if the member does not correct practices as a result of proven complaints.

11. These basic rules apply to all media. They have recently been supplemented by some new CDMA rules respecting consumer privacy online, which are also included in the Code of Ethics and Standards of Practice and subject to the same complaints mediation process. These are designed to protect consumers from unsolicited e-mail, but also state that:

> 'When gathering from individual consumers data that could identify the consumer, and which will be linked with 'clickstream' data, direct marketers shall advise consumers: a) what information is being collected; and b) how the information will be used. The marketer shall provide access to this advisory before consumers submit data that could identify them. Marketers shall also provide a meaningful opportunity for consumers to decline to have information that identifies them collected, or transferred, for marketing purposes. In addition, access to this advisory shall be provided in every location, site or page from which the marketer is collecting such data.'[4]

[4]The term 'clickstream' is defined as data derived from an individual's behaviour, pathway, or choices expressed during the course of visiting a World Wide Web site. http://www.cdma.org/new/ethics.html#Definition

12. Of potential future relevance in the on-line environment is a recent code of conduct from the Canadian Association of Internet Providers (CAIP). A very brief exhortation about privacy states that:

> 'Privacy is of fundamental importance to CAIP members who will respect and protect the privacy of their users. Private information will be disclosed to law enforcement authorities only as requires by law. CAIP members should establish internal procedures to protect personal privacy regardless of the form in which such information is stored, and taking into account the relative sensitivity of each type of information.'[5]

Purpose Limitation, Transparency and Opposition

Collection

13. OH! CANADA collects name, address, day and evening phone numbers, and credit-card number, and holds that purchasing history on its database. For online transactions, the same information is collected (plus the e-mail address). At no point is a cookie set on the customer's hard drive during online transactions. There is no written statement describing the purpose for the collection of personal information. It seems, however, that the company collects only enough information to fulfil the orders submitted, and from these data much can be inferred about the customer's demographic and psychographic profile, though none of these inferences will actually be recorded by the company.

Use of Personal Information for OH! CANADA's Purposes

14. OH! CANADA uses its subscription information to promote its own products from time to time through a separate direct-mail agency. When OH! CANADA conducts its own promotions, it will take steps to ensure that it does not market anybody on its 'Do Not Promote' list. The direct-mail agency that sends out packages of promotions will also have its own 'Do Not Mail' list and may also use the CDMA's 'Do Not Mail, Do Not Call' list.

Disclosure of Personal Information to Third Parties

15. OH! CANADA is a list owner and it rents its list of subscribers to list renters, such as other magazines, non-profit groups and so on. The typical process of list-renting is as follows: Let us say a list renter (perhaps a travel magazine) in the United Kingdom wishes to offer a promotion of its product to British citizens and wants a list of likely customers in Britain. It will contact a list broker in the United Kingdom who will shop around by contacting certain list managers who are responsible for the promotion of the lists of list owners such as OH! CANADA. OH! CANADA's list manager is located in Toronto for the subscribers in its Canadian file, and in Nebraska for those in its international file. Twice a year it provides its list managers with an updated subscriber and customer list.

16. The list manager will contact the list owner to obtain the owner's permission to rent the list and to discuss the terms. These discussions will typically involve the price and the reputation of the list renter; OH! CANADA will sometimes refuse use of its list if it has doubts about the reputation of the business making the request. The list manager might also have questions about how the list should be segmented. The most typical variables for segmentation will be demographic data (which can often be inferred from the postal code), gender, recency of purchase, frequency of purchase, average amount of purchase, and how the customer ordered the product. The list manager will often have questions about how best to segment according to the needs of the list renter, and will consult the list owner on such questions.

---

[5] http://www.caip.ca/caipcode.htm

17. Instructions then go to those responsible for managing the database. For OH! CANADA's Canadian file (located in Toronto), the company responsible for promoting the list and maintaining the data services is one and the same. For its international file, however, it contracts with another company (located in Maryland) for the maintenance of its database. This company then segments and processes the data as requested by the list manager and ships the resulting tape to the list broker in the United Kingdom, who may receive as many as 20 other segmented lists from other sources. They (or the data-processing company with whom they contract) then proceed with a process that has come to be known as 'Merge and Purge'. They merge the files, and will purge them internally of duplicate names and addresses. They will also purge externally by comparing the file against the 'Do Not Mail, Do Not Call' lists maintained by organisations such as the CDMA, or in Britain by the Mail Preference Service. They may also enhance and refine lists against other public and private databases, and will flag names appearing on multiple listings as potentially good customer prospects. The list broker will also include 'dummy' names and addresses in the file. This is to ensure that the list renter does not use the list for more than the one promotion that has been contracted.

18. Consumers are notified of OH! CANADA's list-renting practices in two ways. At the back of the magazine appears this statement: 'Privacy requests are honoured for subscribers who do not wish to receive unsolicited mailings from other companies.' The onus is placed on subscribers to contact OH! CANADA to have their names removed. As many of the overseas subscriptions are purchased by friends and relatives living in Canada, it is doubtful that a foreign customer would have the knowledge of this provision or the ready means to object to disclosures. In the order form for the catalogue items, however, a more explicit 'opt-out' provision is included: 'Occasionally we exchange mailing lists with other catalogues and organisations. If you prefer not to receive their mailings, please check the box.'

19. Although OH! CANADA is not a member of the CDMA, this statement is consistent with the requirements in the CDMA's Privacy Code, which is part of the CDMA's Code of Ethics and Standards of Practice and binding on members of the association.[6] These notices are not, however, available online.

20. OH! CANADA has never faced a situation where its data were requested by governmental agencies, and it is difficult to see the circumstances under which that might happen. All such requests should legally be supported by warrant or subpoena, without which OH! CANADA could potentially be open to an action for breach of confidence.

21. The banks which receive information in the course of approving payment for goods from OH! CANADA by credit card are not currently subject to any data protection legislation in relation to that information. They will be covered by Bill C-54. They also adhere to the common-law duty of confidence. A 1996 Canadian Bankers Association Code of Practice also applies the ten principles of the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information to customer information. A system of banking ombudsmen receive complaints and resolve disputes.

Data Quality and Proportionality

[6]Canadian Direct Marketing Association, *Code of Ethics and Standards of Practice*, at: www.cdma.org/new/ethics.html. Consent provisions are also required by Principle 3 of the Canadian Standards Association's *Model Code for the Protection of Personal Information* (Rexdale: CSA, 1996), so long as non-sensitive data are being transferred. The disclosure of sensitive data requires express consent under the rules of both the CDMA and CSA.

22. OH! CANADA's personal-data collection is driven by a set of basic needs to fulfil an order on time. The information collected and held is typical of the catalogue and magazine marketing business in North America.

23. OH! CANADA typically separates its database according to active versus inactive customers. Both types might be of interest to potential list renters. However, they do not collect information on those who have merely contacted, or made enquiries to, OH! CANADA about their products or services, or who have mistakenly contacted them to find out about current tourist and recreational opportunities in Canada.

24. There are no externally imposed limits for the accuracy, relevance, timeliness and completeness of personal data held by private sector organisations in British Columbia. Nor are there are externally imposed disposal requirements or time limits for retention. OH! CANADA does not have an internally developed retention schedule. When OH! CANADA's lists are rented to other organisations, they are provided for a specific promotion only. Contracts are supposed to ensure that the lists are not used for further purposes, and dummy names and addresses are often included in order to track further unauthorised uses. How successful these practices are cannot be objectively evaluated.

Security

25. Similarly, any security requirements are imposed by internal company policy than by law or by industry codes of practice. Access to the customer database is password-protected, and nobody except current employees of OH! CANADA can have access. OH! CANADA cannot, however, point to any other mechanisms to ensure that employees do not misuse the information under their control, and particularly the credit-card numbers of the portion of its customers who order by credit card. No confidentiality agreements appear to exist. OH! CANADA has never implemented information audit trails, and evidently has no training procedures for employees or written statements of security policy.

26. OH! CANADA's customer database is housed on a different server from that of its website, however. Theoretically, therefore, the customer database cannot be 'hacked' from the outside. Its website is located on a server operated by BC Tel, the major telecommunications operator in the province. Individuals wishing to purchase online can only submit their personal information in unencrypted form. The fact that the site is insecure is currently quite typical of on-line commercial sites in Canada. Recent research in the province of Quebec demonstrated that of 866 corporate websites that permitted on-line transactions, only 26 (about 3 percent) offered the option for secure transactions.[7]

Access and Rectification

27. No law or code of practice obliges OH! CANADA to give individuals access to the personal information it holds on them. The CDMA Guidelines would require such a practice if OH! CANADA were a member. These Guidelines endorse the right of consumers to know the source of their name when used in any direct-marketing programme. Marketers are expected to make all reasonable efforts to provide this information to the consumer on request. Consumers also have the right to know what information is held in their customer files and the right to request correction of any erroneous information.

28. Although OH! CANADA is not a member of the CDMA, it abides by these principles on a voluntary basis. There is no corporate reason why it would not want to honour access requests and correct any information that is inaccurate.

[7] 'Les Enterprises Quebecoises sur Internet', at: http://www.fortune1000.ca/avril98/etude.html

Onward Transfer Restrictions

29. Given that OH! CANADA's international list is held by a company in Maryland, OH! CANADA regularly transfers personal information to another jurisdiction. The relationship between list owner, list manager, list broker and list renter is, of course, strictly controlled by contract. These personal data have value to all in the chain, and so economic incentives dictate a certain level of security for lists such as these.

30. However, at the moment, no provision in British Columbia or federal legislation prevents any private-sector organisation from passing personal information along to jurisdictions with inadequate data protection. Only Quebec's 1993 (Bill 68) addresses situations similar to those in this case. Section 23 states that: 'A person carrying on an enterprise may, without the consent of the persons concerned, use, for purposes of commercial or philanthropic prospection, a nominative list of his clients, members or employees. Every person having such as list for such purposes must grant the persons concerned a valid opportunity to refuse that the information concerning them be used for such purposes.' Section 17 places a statutory duty on enterprises to ensure that a 'valid opportunity to object' is provided before entrusting a person outside Quebec with nominative lists. If operating in Quebec, OH! CANADA would be required to provide a more explicit opt-out opportunity than that included in its current publicity.

Remedies

31. For members of the CDMA, the privacy code is a part of the Association's Code of Ethics and Standards of Practice. This states that 'upon receipt of a customer complaint regarding violation of this Code, *whether regarding a member or a non-member*, the Association will contact the company and use its mediation procedures to attempt to resolve the consumer complaint' (emphasis added). After a process of review and hearings by CDMA, any members found to be in violation will have the opportunity to correct their practices. If further complaints are proven justified, the CDMA board will expel the company from the Association and make a 'broad public announcement that it has done so.' To date, the threat of expulsion has only been used in one case in order to force a company to correct its practices. It is not clear that any sanction could apply to a non-member found in violation of the code. In addition, all CDMA members are expected to designate a staff manager responsible for adherence to the code. The CDMA does not, however, perform a more pro-active auditing role.

32. British Columbia is one of six provinces to have created in statute a cause of action for privacy invasion (Privacy Act, R.S. British Columbia 1979, c. 336). The Act creates a tort for a person 'wilfully and without claim of right, to violate the privacy of another.' The statute goes on to qualify this right in a number of respects, and provides both 'public interest' and 'fair comment' defences. Section 3 of the Act also declares that 'it is a tort, actionable without proof of damage, for a person to use the name or portrait of another for the purpose of advertising or promoting the sale of, or other trading in, property or services, unless that other, or a person entitled to consent on his behalf, consents to the use for that purpose.' A plaintiff seeking to establish this 'appropriation of personality' tort must prove that the defendant specifically intended to exploit the plaintiff's name or reputation.

33. In the 30 years since this tort was established, it has received very little judicial consideration. Most cases relate to instances of intrusion or surveillance, or to the wrongful appropriation of a name or likeness of an individual by the media. The only case that relates to a direct-marketing context occurred when a local furniture retail outlet released the name and address of a woman customer to her ex-partner, who then subjected her to harassment and stalking. However, this and other statutory torts have been notoriously difficult to use for Canadians, let alone for foreign nationals.

Accountability

34. OH! CANADA is audited once a year by the Canadian Circulation Audit Board, chiefly in order to ascertain whether they are making an accurate claim about circulation levels, information of critical importance to advertisers. As a part of this audit, the accuracy of customer information, including names, addresses and source of subscriptions, is checked. This can go some way to improving data quality and proportionality, although these audits do not extend to security questions.

35. Any perceived problem with companies such as OH! CANADA that came to the attention of Canadian or overseas Privacy Commissioners could also be addressed with the encouragement of the company to register under the CSA's Model Code for the Protection of Personal Information. This registration would require a compliance-monitoring process of the kind described under the Canadian case about subcontracted data-processing.

Conclusions

36. In summary, whether online or offline, the handling of personal information collected at the time of purchase of goods or services is a largely unregulated activity in British Columbia, and in most other Canadian provinces. Companies can therefore process, profile, match and use personal information for a range of purposes, including marketing, without the knowledge or consent of the consumer. Only in Quebec is there a general data protection law that imposes fair information practices on companies like OH! CANADA and provides for a method of complaints resolution and redress involving the supervisory authority

37. If a company is a member of the CDMA, then it will be expected to abide by a fairly stringent privacy code under penalty of expulsion from the association. The CDMA operates a complaints-resolution and mediation service, which may be used by overseas customers, but which rarely (if ever) has been. Other self-regulatory mechanisms are currently being developed to apply specifically to online consumer transactions.

38. For companies that are not members of the CDMA, the assessment of adequate data protection must rely on the analysis of individual business practices. Companies like OH! CANADA, although not members of the CDMA, may tend to abide by some basic fair information practices from a sense that responsible businesses practices demand adherence to certain privacy standards. However, the list-rental practices in this case are not as transparent and consensual as would be demanded under the EU Data Protection Directive.

39. However, the desire by the federal government to promote electronic commerce will probably raise the standards for privacy protection in the years ahead. It is no accident that the federal privacy initiative (Bill C-54) has been guided by the Task Force for Electronic Commerce, and that the development of better privacy and security safeguards is widely seen as necessary for Canadians to compete in the knowledge-based economy of the 21st century.

Data in Electronic Commerce

(c) *Hong Kong*

The Nature and Circumstances of the Transfer

1. DRAGON SECURITIES is a Hong Kong securities dealer which has set up an Internet facility to allow users to invest in the Hong Kong Stock Market. Customers registering with DRAGON have an account set up for them; a minimum initial balance of HK$15,000 is required. They can then send trading instructions to DRAGON to buy or sell securities on their behalf, monitor their transactions in real-time, check their portfolio balances, and sign-up for a variety of additional information sources. The Internet trading facility has been in operation since early 1998. Boom client funds are held exclusively in a legally registered 'trust' account at a leading Hong Kong bank, the FIRST ORIENT Bank.

2. DRAGON welcomes overseas investors. This case study looks at the hypothetical use of the DRAGON facility by an investor based in a country in the European Union (EU). Both in setting up an initial account and in conducting transactions, there is clearly a transfer of personal data into Hong Kong, and DRAGON maintains a customer database recording the individual transactions, the customer's current investment portfolio, and the estimated value of the investments at current market prices.

3. DRAGON SECURITIES is a privately-owned securities dealer, established in 1997 and registered with the Securities and Futures Commission of Hong Kong. It is not a member of the Stock Exchange of Hong Kong; it uses an electronic routing system to transmit buy/sell requests to a network of local brokers for efficient execution. Subject to regulatory approval, DRAGON intends to become a regional hub for local securities transactions throughout Asia.

Overview of the Regulatory Environment For This Case

4. DRAGON is subject to the Hong Kong Personal Data (Privacy) Ordinance, and must comply with the six data protection principles. The Ordinance is a comprehensive data protection law covering both the private and public sector, and establishing the Office of the Privacy Commissioner for Personal Data to administer and enforce the law. The Commissioner has issued specific guidance for data users collecting, displaying or transmitting personal data over the Internet (*Personal Data and the Internet - a Guide for Data Users*, January 1998). If DRAGON was a credit provider, which it appears not to be, it would also be subject, from 27 November 1998, to the Code of Practice on Consumer Credit Data issued by the Commissioner in February 1998.

5. DRAGON is also subject to the laws governing Hong Kong's financial markets which impose certain requirements affecting the level of privacy protection enjoyed by DRAGON's customers. The main regulator with jurisdiction over securities dealers is the Hong Kong Securities and Futures Commission (SFC), which issued Management, Supervision and Internal Control Guidelines ('the Guidelines') in 1997 as a supplement to an earlier and rather broadly-worded Code of Conduct.

6. The Hong Kong Direct Marketing Association has a Code of Practice for the use of Personal Data in Direct Marketing. It is not a statutory code like the Consumer Credit one, but gives guidance to members on how to comply with the terms of the Privacy Ordinance in the context of direct marketing activity. However, DRAGON is not currently a member of the HKDMA.

Purpose Limitation, Transparency and Opposition

Collection

7. Collection of personal data by DRAGON first takes place when someone applies to open an account. There appear to be no attempts to install cookies on an Internet user's computer when they are just browsing DRAGON's website for information.

8. Prospective customers have a choice of application methods: they can complete and submit an application form online, or print one off and send it by mail or fax. There are two forms, one for an individual account and another for a joint account. Both ask for a range of personal details, some of which are clearly marked as mandatory (if applicable). These include, as personal information, names, gender, data of birth, marital status, official ID or passport number, citizenship and country of residence, and, as contact information, telephone numbers, e-mail and postal addresses. The only information requested which is clearly voluntary is occupation, but no explanation is given as to why this might be required.

9. Applicants are required to provide copies of their ID card or passport ID page, and at least one official item of proof of address. These are presumably required to meet Hong Kong government requirements, although this is not explained. A signed client agreement is also required to establish a legal contract between the applicant and DRAGON.

10. Payment to establish the initial account can be made either by telegraphic transfer or by sending a cheque or bank draft. Customers are also required to provide bank contact information for continuing transfers of funds. Subsequent deposit and withdrawal of funds from the FIRST ORIENT bank account can be made by the same means, but hard copy confirmation of all such deposits and withdrawals still have to be sent by the customer to DRAGON to meet legal requirements

11. Once an account is opened, customers are given access to a 'virtual dealing room', where they can view stock market information - provided online by an associated information service - for an additional fee. They can send trading instructions either online or by phone or fax, and these are carried out on their behalf by one of a number of associated brokers, with the purchase or sale being confirmed online, and in a monthly account statement.

12. DRAGON's client agreement, which customers are required to sign and return, is available online in both the English and Chinese languages. It includes some information about personal information, although it is not brought together in a privacy or information-management section. The agreement authorises DRAGON to obtain bank references and carry a credit check 'for the purpose of ascertaining…financial situation and investment objectives', and to 'disclose information…to any department or agency of any government or public body… on request to assist any of them with any investigation or enquiry…whether or not such request is legally enforceable.'

13. This notice falls short of what is required by the Privacy Ordinance (DPP5 and DPP1(3)). For example, in relation to DPP5, the statement does not specify the types of personal data held by DRAGON, nor the purposes for which it uses the data. In relation to DPP1(3), there is, for example, no notification of the individual's rights of access and correction and whom to approach to exercise these rights.

Use and disclosure for DRAGON's purposes

14. DRAGON uses the customer information to create a trading account on their system for each customer. Instructions to buy or sell particular shares need to be disclosed to the

broker (selected on each occasion by DRAGON), but the identity of the client is not disclosed.

15. As noted above, DRAGON indicates in its client agreement that it will take up bank references and undertake credit checks on new applicants. Credit checks with a credit reference agency will from 27 November 1998 be subject to the provisions of the Code of Practice on consumer credit data issued by the Privacy Commissioner for Personal Data in February 1998. This Code complements the Personal Data (Privacy) Ordinance and gives guidance to lenders about how compliance with the data protection principles of the Ordinance will be assessed in the context of credit information. It is not apparent that DRAGON is offering its customers 'credit' as defined in the Code of Practice and it would not therefore be allowed under the Ordinance to make enquiries of a credit reference service, even with the customer's consent. The Ordinance and Code would not prevent DRAGON from taking up references from other banks or individual lenders.

16. There is no indication in the client agreement or on the website as to what if any other uses DRAGON may make of customer information, such as marketing offers of financial services and products. Since DRAGON is not a member of the Direct Marketing Association (HKDMA), it cannot be assumed that it follows the detailed guidelines set out in the Association's code of practice. However, under s.34 of the Hong Kong Ordinance, DRAGON would have expressly to notify customers of any proposed direct marketing, and to offer them the opportunity to opt out.

17. There will be routine disclosures to the FIRST ORIENT Bank as and when DRAGON's customers deposit funds or send instructions for a withdrawal, but since the funds are kept in common trust account, FIRST ORIENT never has personal information about individual DRAGON clients. In any case, the bank is subject to the same requirements of the Privacy Ordinance as DRAGON and has additional common-law obligations of confidence to all its customers.

Disclosure to third parties for other purposes

18. As indicated in the client agreement cited above, DRAGON asserts the right to make disclosures of personal data to any government or public body. Under other Hong Kong laws, various government officials have a statutory right to information upon demand; e.g., law enforcement bodies can obtain warrants in the course of investigations.

19. If DRAGON's actual policy is simply to disclose on request to any government or public body asserting that they are conducting an investigation, then this would seem to be in conflict with their obligation under Data Protection Principle (DPP)3 only to use (disclose) personal data in certain defined circumstances. These circumstances include those where disclosure is required by law, and where they have reasonable grounds to believe that the use (disclosure) would be likely to prejudice one of a range of law enforcement and revenue protection functions (s.58). But in order to take advantage of this latter exception, the data user would arguably have to do more than DRAGON's statement suggests they would do to satisfy itself.

20. Nearly all potential recipients of personal data in Hong Kong will themselves be data users subject to the Privacy Ordinance, so the data will continue to have the same external protection as they enjoy when they are held by DRAGON, having regard to the 'authorised' uses which recipients may be able to make of the data; for many government agencies this will be set out in other laws.

Data Quality and Proportionality

21. The Hong Kong Privacy Ordinance requires data users to ensure that personal data are accurate (DPP2). DRAGON relies heavily on customers themselves to ensure the quality of factual personal information, with clauses in the client agreement placing the responsibility on the customer to notify DRAGON of any changes or errors. The onus of

responsibility for checking that trading instructions have been accurately carried out is placed on clients, with a requirement that they notify DRAGON within two days of receipt of confirmation of any error (and notify DRAGON if they do not receive confirmation). This attempt to limit DRAGON's liability for accurate, complete and up to date data may well not be lawful, and it is likely that if a customer could clearly show that DRAGON were at fault and responsible for some data quality error, then DRAGON could be found to be in breach of the Ordinance, notwithstanding the contract term. DRAGON also seeks in the client agreement to escape liability for any risk resulting from the use of the 'inherently unreliable' medium of the Internet. This too may not be consistent with their obligations under the Ordinance. It is fair enough to warn customers of the risks, but who is liable for the consequences of any Internet-related problem would have to be judged on the merits of the particular case.

22. The 'frequently asked questions' (FAQ) on security on DRAGON's website says that for security reasons, personal details about customers, such as mailing addresses and bank details, are kept on a separate computer and are therefore not available to be checked by customers online, although they are able to see their account balances and transaction history. This reassurance appears to conflict with another FAQ which tells customers that they can make their own changes to the 'Contact Information' online, although these could be consistent if the online facility simply notifies DRAGON, which then makes the requested changes on the other system.

23. DPP2 of the Hong Kong Ordinance forbids data users to keep personal data for any longer than is necessary for the fulfilment of any legitimate purpose. This should lead organisations to review their data management practices and institute record disposal programmes. It is not clear if DRAGON has instituted such a programme.

Security

24. The Hong Kong Ordinance requires data users to take all practicable steps to protect personal data against unauthorised or accidental access, processing, erasure or other use (DPP4). DRAGON emphasises security in all its publicly available material. It is clearly seen by the business as an essential selling point, given the sensitivity of financial services customers to issues of confidentiality, integrity and security against unauthorised access.

25. DRAGON states in the FAQ pages of its website that it addresses security at four levels. Level 1 is the requirement for a unique customer ID and customer-selected password for access to the DRAGON facility. Level 2 requires a separate personal identification number (PIN) to access the 'virtual dealing room' to send instructions to buy or sell securities. Level 3 is the use of encryption for all communications (no details of the level of encryption employed are given in the public section of the website). Level 4 security is provided through the separation of a client's personal details, such as bank details and mailing addresses. These are kept off-line in a separate computer from the one that handles the trading account information and virtual dealing room; but see comments, above, on online changes of contact details.

26. In addition, written confirmation is required before withdrawals can be made from customers accounts. The form of trust account used by DRAGON to hold funds at the FIRST ORIENT Bank prohibits a broker from transferring or accessing client funds for any purpose other than buying or selling on behalf of its clients. For each transaction in relation to a 'trust' account, a detailed record must be kept to prove to government auditors that no misappropriation has taken place. These records are maintained by DRAGON, and FIRST ORIENT never receives information about individual customers.

Access and Rectification

27. The Hong Kong Privacy Ordinance creates a right of access for individuals to information about themselves, subject to a range of exemptions, and provides correction rights and a process for challenging refusal of access (DPP6). However, as noted earlier, there is no indication on the DRAGON website that they are aware of these obligations or have a system for handling requests.

Onward Transfer Restrictions

28. Section 33 of the Hong Kong Ordinance will prevent data users from transferring personal data outside Hong Kong unless certain conditions are met, with the aim of ensuring that the data will be continue to be protected and handled in accordance with privacy principles. This Section is not yet in force. The Privacy Commissioner has issued further guidance on this provision (Fact Sheet 1, May 1997).

29. When s.33 is brought into force, data users such as DRAGON will be able freely to transfer data to any places which have been specified by the Privacy Commissioner as having similar laws, without any further steps. It seems likely that European Union member states will be declared to have similar laws, and therefore transfers about a European client back to his or her home country will not pose any difficulty. But if DRAGON wants to transfer information about a client to a 'third' country which has not been specified, it will only be able to do so if:

- it has reasonable grounds for believing that there is a similar law in force (in the absence of any guidance from the Privacy Commissioner);
- it has obtained the client's consent in writing;
- it is in her interests but in circumstances where consent is impracticable to obtain (but likely);
- the use or disclosure involved is an exempt one for the purposes of DPP3, or
- the data user has taken reasonable precautions and exercised ‘all due diligence’ to ensure the data will be handled responsibly.

Fact Sheet 1 suggests that one way of demonstrating 'due diligence' is to use contract terms, and a model contract is included.

30. In the DRAGON case, transfers of personal data to third countries would be most likely where a client instructs DRAGON to buy or sell securities in a third country financial market. While this service is not currently available, DRAGON intends to offer it as soon as practicable.

31. The inclusion in the Hong Kong law of an 'onward transfer' provision, similar in terms and effect to Articles 25 and 26 of the EU Directive, would appear to satisfy one of the core requirements which EU members are likely to require in order to assess a place as having adequate protection, once s.33 is in force. The breadth of the DPP3 exemptions as applied to s.33 would seem at first sight to weaken the effectiveness of s.33 as a safeguard, but are in fact analogous to the exception provided by Article 26(1)(d) of the Directive.

Remedies

32. Under the Hong Kong Privacy Ordinance, individuals can complain to the Privacy Commissioner about alleged breaches of any of the privacy principles. This right applies to any individual about whom data are held; they do not have to be Hong Kong citizens or even residents. A foreign national such as one of DRAGON's customers in this case study would clearly enjoy all the rights given to individuals under the Ordinance.

33. The Commissioner's staff can assist the complainant and try to mediate. If this is unsuccessful, an investigation can lead to the Commissioner's issuing an enforcement notice, directing the data user to take specified action, and/or instigating prosecution action. Contravention of an enforcement notice is an offence which can result in a fine or imprisonment. The Ordinance creates a right of action for compensation for damage or distress, although individuals would have to bring such action in the civil courts.

34. Some privacy breaches may also be breaches or offences under other laws, and other remedies and penalties may apply.

Accountability

35. DRAGON SECURITIES does not advertise any specific chain of accountability for compliance with those aspects of confidentiality and privacy that are addressed in its stated policies. Like most small and medium sized businesses, it tends to calculate its risks in deciding how far to comply with legislative requirements. The requirements arising from financial services regulation, being longer established and better known, receive the highest priority. Businesses in Hong Kong are still learning about the Privacy Ordinance and its obligations.

36. DRAGON's policy of client confidentiality is emphasised in routine training for employees**.** Security in particular is emphasised, and each employee signs a non-disclosure agreement. Misuse of customers' personal information of customers would result in the dismissal of an employee.

37. Securities dealers in Hong Kong are subject by law to annual external audits and potentially to compliance inspections by the Securities and Futures Commission.

38. The Privacy Commissioner also has a pro-active monitoring role under the Ordinance and proposes to commence a programme of inspections (audits) later in 1998.

Conclusions

39. The Hong Kong Personal Data (Privacy) Ordinance has established a legal regime in which all organisations handling personal data in Hong Kong are required to comply with a set of data protection principles similar in most respects to those in the EU Directive and member states' laws. Individuals, including foreign nationals, have legal rights under the Ordinance. The Ordinance has also created a comprehensive system of supervision, compliance monitoring and enforcement through the Office of the Privacy Commissioner for Personal Data.

40. Once the onward transfer provisions of s.33 are in force, the privacy protection regime in Hong Kong as it applies to the handling of personal data collected through the Internet by a business operating in Hong Kong in its own right would appear to be adequate for the purposes of Article 25. The same applies to the consequential processing of personal data by the FIRST ORIENT Bank.

41. However, a significant issue that this case raises is the extent to which the mere existence of a privacy or data protection law can be taken to ensure adequate privacy protection. There is evidence in this case that organisations such as DRAGON may not yet be complying with all the requirements of the Ordinance. Given that the law is still relatively new, and that the Commissioner is still engaged in activity to create awareness of obligations, this could arguably be expected, and it need not invalidate a general conclusion that the framework should ensure adequate protection as it becomes better known and is implemented. The important point is that businesses such as DRAGON are liable for any

breaches of the Data Protection Principles, and that comprehensive and easily accessible remedies are available.

Data in Electronic Commerce

(d) *Japan*

The Nature and Circumstances of the Transfer

1. RISING SUN Books is a leading book retailer in Japan and a large exporter of Japanese publications and English-language books about Japan. It also deals in periodicals, electronic information products, microfilm, music, audio-visual materials, language tutorials as well as rare and antiquarian books. It has around 50 stores in the major cities in Japan, and around 30 overseas. In its 70 years in existence, RISING SUN has built up a large international network of sales offices and representatives that can service universities, private companies, government, libraries as well as individual consumers. RISING SUN now has customers around the globe.

2. In 1996, RISING SUN opened up its 'virtual bookstore' on the Internet, through which customers can freely search a database of over three million titles, about half of which are in Japanese. The system allows customers to access the website and search for titles. However, they must become members before placing orders. The main database is located on a server in Japan. Depending on the title, books are then delivered within one to three weeks. Some are shipped directly from distributors in the home country. Others may have to be sent by air-mail directly from the RISING SUN distribution centre in Tokyo.

Overview of the Regulatory Environment for This Case

3. No private-sector data protection law governs the operations of RISING SUN. Japanese data protection policy in the private sector currently relies on an encouragement of voluntary self-regulation. Indeed, the Japanese have joined the Americans in promoting the value of self-regulation, at least for non-sensitive data, in opposition to the more regulatory approaches in Europe.

4. The protection of privacy in the Japanese private sector relies mainly, therefore, on a number of sectoral codes of practice that have been developed and published in conformity with a series of guidelines from the Ministry of Trade and Industry (MITI), the most recent of which was published in March, 1997 ('Guidelines Concerning the Protection of Computer Processed Personal Data in the Private Sector') and which takes into consideration the provisions of the European Union (EU) Data Protection Directive.

5. Two sets of guidelines relate to electronic commerce. In December, 1997 the Cyber Business Association (CBA) published its 'Guidelines for Protecting Personal Information in Cyber Business.' In March, 1998 the Electronic Commerce Promotion Council of Japan published its 'ECOM Guidelines Concerning the Protection of Personal Data in Electronic Commerce in the Private Sector', based on the MITI guidelines (see http://www.ecom.or.jp/ecom_e/). This latter instrument seems more applicable to businesses such as RISING SUN. The analysis for this case therefore focuses on the obligations contained in these Guidelines and compares them with the practices of RISING SUN.

6. The ECOM Guidelines are intended to provide guidance for any business that engages in 'business transactions conducted on electronic networks.' They are generally based on the framework of the 1980 Organisation for Economic Co-operation and Development (OECD) Guidelines, supplemented by certain provisions that appear in the EU Data Protection Directive.

Purpose Limitation, Transparency and Opposition

Collection

7. The ECOM Guidelines (Article 5) contain the familiar stipulation that 'the person using personal data in electronic commerce shall clearly specify, within the bounds of legitimate business, the purpose of collecting such data and shall perform such collection to the extent necessary to achieve such purposes.' The Article is intended to prohibit the 'presentation of false advertisements on screen displays to encourage bogus transactions.' Article 6 stipulates that 'personal data shall be collected by fair and lawful means.' Article 7 prohibits the collection of 'specific personal data of a delicate nature.' Article 8 contains some fairly stringent requirements for the notification to the data subject of: who is the responsible manager of personal data; the purposes for collection; any third party recipients; the effect if certain data are not disclosed; and the existence of a right of access and correction. In the case where personal data are collected directly from a source other than the subject of the data, the data subject shall be notified accordingly and consent obtained. Articles 24 and 25 also contain special provisions concerning the collection of personal data from children.

8. RISING SUN books collects the following information from a customer who orders a book: name, e-mail address, date of birth, gender, postal address, phone number and fax number. Through a drop-down menu, it then asks the consumer to select a credit card for payment and to enter the number, cardholder name and the expiry date. It also asks other questions: how the customer heard about the virtual bookstore, what is the customer's occupation and area of expertise, and what kinds of magazines the customer likes to read. It appears that no cookie is set either during visits or ordering. For the latter, however, the customer needs to enrol as a member. Only a small amount of promotional material is available without membership.

9. Provision of such information seems to be a condition of becoming a member of RISING SUN's Virtual Bookstore. Strict rules are communicated about: informing RISING SUN if personal information changes; sharing or publishing information obtained through the Virtual Bookstore; and allowing others to use one's ten-character password. The kinds of personal information collected by RISING SUN seem excessive, and inconsistent with the stipulations in the ECOM Guidelines.

Use and Disclosure for RISING SUN's Purposes

10. Article 10 of the ECOM Guidelines stipulates that 'the use of personal data shall, in principle, be limited to the purpose of collecting said data with the exception of the case of Article 12 (which obliges organisations to obtain consent for new uses).' In cases where the enterprise might want to use these data in order to promote their own products or services, the Guidelines are clear that the consent of the subject shall not simply be obtained by posting a notification on the screen or through electronic mail, 'but by clearly indicating consent by clicking an 'I consent' button on the screen and receiving a return acknowledgement by electronic mail.'

11. RISING SUN does not give any indication of how it might use personal customer data for its own internal purposes, nor does it provide any opportunity to indicate one's consent.

Disclosure to Third Parties for Other Purposes

12. Article 13 (based on Principle 8 of the OECD Guidelines) limits disclosure of data to the purpose for which they were collected, unless the prior consent of the data subject is obtained. In an electronic-commerce environment, the most typical third-party disclosure is to another enterprise for direct-mail uses. In these circumstances, 'notification shall be

given on screen or in advance and consent obtained.' The Guidelines suggest that a clear choice be given between clicking '1' for I consent, and '2' for I do not consent. The standard for disclosure seems to be 'express' rather than 'implied' consent.

13 RISING SUN asserts that it does not disclose customer information outside the company. However, no notification to this effect appears on its website.

Data Quality and Proportionality

14. Article 16 contains the typical stipulation that 'personal data shall be kept accurate and up-to-date to the extent necessary for fulfilling the purpose of use.'

15. The rules for members place an obligation on the member to provide accurate information and to inform them if circumstances change. Membership in RISING SUN might be cancelled if false information is given. However, it is not clear whether RISING SUN takes other measures to maintain the accuracy and currency of the personal information in their files.

Security

16. Article 17 provides that 'reasonable security measures shall be taken through both technical and organisational means against such risks as unauthorised access to personal data or the loss, destruction, alteration, leakage etc. of personal data.'

17. Orders with RISING SUN occur through a secure server, using a standard and widely used system for secure web transaction. Upon clicking the online server link, the internet browser informs the consumer that a secure document is being requested and that all data transmitted during the ordering process will be encrypted.

Access and Rectification

18. Article 20 of the ECOM Guidelines allows a right of access and 'accuracy verification.' In the electronic-commerce environment, the subject of the data 'must be informed on a computer screen of the right to have personal data presented, corrected or deleted.' It is also suggested that the exercise of this right could be 'performed through on-screen displays or by providing explanations in response to onscreen inquiries.' This does, of course, require a system of authentication. Rights of access and correction should be provided within a 'reasonable period of time'.

19. There is no indication on RISING SUN's website of any of these features. This is not to say that they would refuse requests for access and correction of personal data.

Onward Transfer Restrictions

20. The ECOM Guidelines contain no specific prohibition against onward transfer restrictions beyond those discussed above relating to disclosure limitation.

Remedies

21. The ECOM Guidelines contain no specific provisions for complaints-resolution and redress; the Electronic Commerce Promotion Council of Japan does not provide such a function. 'However, the process of securing remedies, while still in a very fledgling state, seems to indicate that an aggrieved consumer can register a complaint with the Consumer

Consultation Service specialising in personal-data protection within the Japan Information Processing Development Center (JIPDEC), a non-profit organisation supported by MITI and by certain industrial associations. Evidence of privacy invasions may then be communicated to a new sub-committee within the Industrial Structure Council of MITI, an advisory body to the Minister. This evidence might also be used in the granting, or refusal, or 'Privacy Protection Marks' (PPMs), a 'good housekeeping seal of approval' that is intended to permit consumers to distinguish between privacy-friendly and privacy-invasive organisations. In this way, 'businesses that do not provide adequate data protection will be naturally eliminated through the market mechanism', according to a MITI paper of April, 1998 ('Japan's Views on the Protection of Personal Data'). MITI expects this system to be especially effective within the online environment. As at September, 1998, PPMs have been awarded to 16 companies and firms.

22. The Civil Code stipulates that compensation can be awarded for damages arising from any maltreatment by a privact-sector organisation. However, it is very difficult to prove damages resulting from the mistreatment of personal information, especially in 'cyberspace'.

Accountability

23. The ECOM Guidelines stipulate that 'one or more persons shall be designated from those who understand these guidelines and have the capacity to put them into practice.' These 'managers of personal data' shall 'understand and observe the provisions of these guidelines, and shall accept responsibility for causing employees to understand and observe these guidelines by providing training, establishing internal regulations, implementing security measures, establishing a compliance program, and taking measures to ensure that the program is generally known.'

24. RISING SUN has never developed a privacy protection policy, and therefore could not point to any one employee with overall responsibility for the management of personal data, as seems to be required by the ECOM Guidelines. Neither can they point to any external audits of their data-handling practices.

Conclusions

25. The assessment of the practices of RISING SUN suggests that there are certain shortcomings with respect to the collection of excessive personal data, and with respect to the notification given to consumers about collection, use and disclosure policies. This assessment is, however, tentative, but it is instructive about the problems to be anticipated in assessing the adequacy of data protection in Japanese society.

26. The assessment of the adequacy of protection for personal data collected via electronic commerce in Japan is fraught with many difficulties. First, the instruments to which private enterprises are expected to comply are voluntary. As with all such instruments, they tend to affect the behaviour of the responsible organisations and leave the irresponsible untouched. Free-riders can then collect, use and disclose personal information without regard to the constraints within mechanisms such as the ECOM Guidelines.

27. A second difficulty relates to the very recent adoption of many of these measures. The effectiveness of the guidelines, as well as the complaints monitoring and privacy protection mark regime, is impossible to evaluate at this early stage. The idea of 'good housekeeping seals of approval' is an intriguing one that has from time to time been suggested in Canada in association with the operation of the CSA standard. Again, we need a critical mass of organisations in different sectors being awarded the PPM before we can assess whether 'businesses that do not provide adequate protection will be naturally eliminated through the market mechanism.'

28. The ECOM Guidelines, and the associated PPM, are intended to be used by both Japanese and overseas consumers. The Mark itself is written in both Japanese and English and can give a clear indication of those organisations that are ‘privacy-friendly’. Whether or not overseas consumers could do anything more than make a basic marketplace choice between one website and another is, however, doubtful. There are major constraints, not least of which is the ability to discover, understand and use a set of rules, only a portion of which are translated from the original Japanese.

Data in Electronic Commerce

(e) *New Zealand*

The Nature and Circumstances of the Transfer

1. KIWI PRODUCTS is an initiative of New Zealand merchants who have set up a joint Internet facility to market their goods.

2. KIWI welcomes overseas customers, and this case study looks at the hypothetical case of a European customer. Both in setting up an initial account and in conducting further transactions, there is clearly a transfer of personal data about the customer into New Zealand, and KIWI maintains a customer database recording individual transactions.

Overview of the Regulatory Environment for This Case

3. Both KIWI and the participating New Zealand merchants are subject to the New Zealand Privacy Act 1993, which establishes both privacy standards (Information Privacy Principles, or IPPs) and enforcement and complaint mechanisms. After a transitional period, the Act has been fully in force since 1996. The New Zealand Privacy Commissioner has issued a considerable amount of guidance material for businesses on compliance with the Act, and a wide range of training has been offered. The New Zealand Privacy Act makes provision for sector or activity codes of practice which can substitute for the 'default' principles, but there have been no such codes developed that would affect KIWI PRODUCTS' activities.

Purpose Limitation, Transparency and Opposition

Collection

4. Collection of personal data by KIWI PRODUCTS first takes place when someone either places an order or sends an e-mail enquiry to their website. There appears to be no attempt to install 'cookies' on Internet users' computers when they are just browsing KIWI's website for information.

5. First-time customers are asked to provide delivery and payment details, together with an e-mail address. KIWI makes use of proprietary 'shopping basket' software which allows them to browse through the range of products available and add prospective purchases to a 'parcel', choosing quantity and, where applicable, colour and size. The completed 'parcel' can then be checked before submitting the order. Customers are also given the option of gift delivery which can include a card with message, and which does, of course, require a separate delivery address to be entered. Internet customers also specify one of four methods of delivery: surface mail, economy air, first-class airmail or courier.

6. There is also an optional e-mail application form which the customer can use to be placed on a postal mailing list for the KIWI PRODUCTS catalogue, with the option of receiving updates about one or more specific product categories, including the express option of receiving the catalogue but no updates.

7. The KIWI website does not advertise a privacy policy, and apart from the obvious explanation for entering details (i.e., to place an order, receive a catalogue, etc.) there is no detailed attempt to explain what the personal information will, or will not, be used for (see below for assurances about security). For instance, while it is obvious that submitting the mailing list application form will result in mailings, it is not clear whether KIWI

PRODUCTS will also send a catalogue to customers who have placed an order but who have not completed and submitted an application form for the mailing list.

8. Repeat customers are encouraged to apply for a 'Top Customer' number, with the incentive of a NZ$50 credit for each NZ$500 worth of goods ordered. Delivery and payment details are retained for 'Top Customers' so that they do not need to re-enter this information each time; they use a self-selected password to 'call up' their registered details to accompany a new order. Payment options are currently restricted to credit card, requiring the standard details of card type, name, number and expiry date.

9. KIWI's apparent failure to explain why it collects personal information and what it will be used for could constitute a breach of the New Zealand Privacy Act.

Use and disclosure for KIWI PRODUCTS purposes

10. KIWI PRODUCTS uses the customer information to fulfil orders for each customer, and if requested adds the customer's postal address to its mailing list for catalogues. KIWI PRODUCTS will also carry out the usual merchant authorisation check of the customer's credit card details. These uses and disclosures would appear to meet the requirements of IPPs 10 and 11, being either part of the original purpose for which the information was collected, or a directly related purpose.

Disclosure to third parties for other purposes

11. KIWI PRODUCTS does not sell or rent its list of customers to third parties, although the participating companies do have access to the list of all customers, not just those that have ordered their products. KIWI is a member of the New Zealand Direct Marketing Association which has some clauses relating to personal information in its 'standards of practice' which reflect the Privacy Act requirements. If KIWI or any of the participating merchants decide in future to offer customer lists for sale or rental, then to comply with the New Zealand Privacy Act they would need to seek the consent of each customer, since this intention was not communicated to them when the information was collected. This would need to be an affirmative authorisation (opt-in); KIWI could not simply notify customers and rely on them not objecting (opt-out).

12. Under New Zealand law, various government officials have a statutory right to information upon demand; for example, law-enforcement bodies can obtain warrants in the course of investigations. Although the activities of KIWI PRODUCTS are unlikely routinely to attract the attention of the authorities, it is conceivable that tax, customs or police agencies may seek information about particular customers from KIWI PRODUCTS.

13. There is nothing on KIWI PRODUCTS' website to indicate how they would react to any such request. If they simply disclosed personal information on request to any government agency or public body asserting that they are conducting an investigation, this would seem to be in conflict with their obligation under IPP 11 to disclose personal data only in certain defined circumstances. These circumstances include where disclosure is necessary to avoid prejudice to one of a range of law-enforcement and revenue-protection functions. If KIWI PRODUCTS received a valid warrant or subpoena for information, then they would not be expected to enquire further, but other 'informal' requests would require KIWI PRODUCTS to take reasonable steps to satisfy themselves as to the *bona fides* of the requester and the necessity for the release.

14. Nearly all potential recipients of personal data in New Zealand, including public authorities, will themselves be 'agencies' subject to the Privacy Act, so the data will continue to have the same external protection as they enjoy when they are held by KIWI PRODUCTS, having regard to the 'authorised' uses which recipients may be able to make of the data; for many government agencies, these will be set out in other laws.

Data Quality and Proportionality

15. The New Zealand Privacy Act requires data users to ensure that personal data are accurate, up to date, complete, relevant and not misleading before using it (IPP 8).

16. KIWI PRODUCTS relies on customers themselves to ensure the quality of factual personal information. Given the relatively low risk of harm or damage which would arise from any errors, this would almost certainly be held to be 'reasonable' in terms of the IPP 8 requirement.

17. IPP 9 of the New Zealand law limits data users from keeping personal data for any longer than is required for the purposes for which it may lawfully be used. This should lead organisations to review their data management practices and institute record disposal programs.

Security

18. The New Zealand Privacy Act requires agencies to adopt reasonable security safeguards to protect personal information against loss and unauthorised access, use modification or disclosure (IPP 5).

19. KIWI PRODUCTS emphasises security on its website, offering customers the choice of standard or secure servers to transmit their orders. The website explains that the secure server encrypts all information associated with an order in transmission, and that the credit card number is 'locked away' in a separate computer which is not connected to the Internet. However, KIWI PRODUCTS also attempts to reassure customers that it is safe to use the standard server, quoting from a newspaper article about the security of giving credit-card numbers by Internet relative to other ways of using cards. There is presumably a cost saving to KIWI PRODUCTS that leads them to offer the choice**.**

Access and Rectification

20. The New Zealand Privacy Act also confers access and correction rights (IPPs 6 and 7), on citizens and others in the country, but these particular rights expressly do not apply to non-residents outside New Zealand. A European customer could not therefore make an access request from Europe. Although there is no express reference to these rights on the KIWI PRODUCTS website, there is no reason to believe that they would not normally comply with these provisions in respect of any customer making a formal access request or requesting correction of any details. While a non-resident overseas could not insist on these rights, or seek redress through the Privacy Commissioner, KIWI may well make them available to him as a matter of company policy.

Onward Transfer Restrictions

21. There is no obvious reason for KIWI PRODUCTS to need to transfer personal information about customers outside New Zealand. If it did so, perhaps for data processing or hardware or software maintenance, the question of offshore protection arises.

22. The New Zealand Privacy Act does not currently contain any provisions which restrict the transfer of personal data outside New Zealand. The Commissioner, in his recent review of the Act, invited submissions as to whether such a provision was needed (partly in light of Article 25 of the European Union (EU)). The Commissioner is expected to issue his report on the Review in October. However, this is unlikely to be a relevant issue in this case study.

23. While there is no express 'onward transfer' provision in the Act, two other provisions in the law are relevant. Section 10 of the Act applies all of the relevant principles

(5 to 11) to information held outside New Zealand by a New Zealand agency, although an additional 'exception' is granted to the non-disclosure principle for any action that an agency is required to take by or under any law of an overseas jurisdiction. IPP 5 also requires agencies, when disclosing information in connection with the provision of a service, to take reasonable steps to prevent unauthorised use or disclosure. In deciding whether KIWI PRODUCTS or any other agency was still in control of any personal information transferred outside New Zealand, the terms of any contract would be relevant.

Remedies

24. Some larger businesses in New Zealand, and most government agencies, have formalised internal complaints mechanisms, but most small and medium-sized enterprises such as KIWI PRODUCTS would only be expected to handle customer complaints as a normal part of customer service.

25. Under the New Zealand Privacy Act, individuals can complain to the Privacy Commissioner about alleged breaches of any of the privacy principles, or of the procedures relating to requests for access or correction. This right applies in most cases to any individuals about whom data is held; they do not have to be New Zealand citizens or even residents, with the exception that the access and correction rights (IPPs 6 and 7) do not apply to non-residents unless they are actually in New Zealand.

26. With this exception, a foreign national would enjoy all the rights given to individuals under the law. The Commissioner's staff could assist a European customer of KIWI PRODUCTS and try to conciliate or mediate his complaint. If this is unsuccessful, the Commissioner can refer the matter to a separate Proceedings Commissioner, who will in turn decide whether to take the case to the Complaints Review Tribunal. The Tribunal can make an order prohibiting a repetition of the action complained about, and/or require the interference with privacy to be put right. The Tribunal can also require the respondent agency to pay damages or compensation.

27. It should be noted that very few complaints proceed as far as the Tribunal - most are resolved at an earlier stage. Also, there is a substantial complaints handling backlog due to resource constraints, with individuals typically having to wait twelve months for investigation of their matter to even begin, unless it is assessed as urgent.

Accountability

28. After five years, most businesses in New Zealand should be at least generally aware of the Privacy Act and its obligations. Section 23 of the Privacy Act requires agencies to designate someone within the organisation as Privacy Officer to deal with privacy matters. KIWI PRODUCTS does not advertise any specific chain of accountability for compliance with its assurances about confidentiality. Like most small and medium-sized businesses, it tends to calculate its risks in deciding how far to comply with legislative requirements.

29. KIWI PRODUCTS' policy of client confidentiality is emphasised in routine training for employees. Security in particular is emphasised, and each employee signs a non-disclosure agreement. Deliberate misuse of personal information of customers would result in disciplinary action, and, if serious enough, in the dismissal of an employee.

30. The Privacy Commissioner has no express audit or inspection powers under the Privacy Act outside the investigation of complaints, and conducting audits on request, but does have a function to enquire generally into any matter, including any law, practice, or procedure in the private or public sector. The Privacy and Proceedings Commissioners, and the Complaints Review Tribunal, are independent statutory appointments at arm's length from government.

Conclusions

31. The New Zealand Privacy Act 1993 has established a legal regime in which nearly all organisations handling personal data in New Zealand are required to comply with a set of data protection principles similar in most respects to those in the EU Directive and member states' laws. Individuals, including foreign nationals, have a range of entitlements under the law. The Act has also created a comprehensive system of supervision and enforcement through the Privacy Commissioner (lacking only a pro-active audit role), and an associated complaints review machinery.

32. Personal information about European customers of businesses such as KIWI PRODUCTS, trading over the Internet, is therefore protected by law in a way which in most respects meets the test of adequacy envisaged by the Article 29 Working Party in relation to Article 25 of the EU Directive. The only limitation on a non-resident's rights relative to a New Zealand citizen or permanent resident is that he or she cannot make an enforceable access or correction request from outside the country. The absence of a comprehensive onward transfer provision in the law would only be an issue in this case study if personal information about a customer was sent on to a third country without his consent, and this seems unlikely.

33. An issue raised by the KIWI PRODUCTS case is the extent to which the mere existence of an adequate privacy or data protection law can be taken to ensure adequate privacy protection. On the positive side, the Privacy Commissioner's office is active in promoting the law and handling complaints (although the complaints backlog is disturbing); cases have progressed through the mechanisms to the courts in some instances, and remedies have been provided for breaches of the law, including the payment of compensation.

34. However, it appears that KIWI PRODUCTS may not yet be complying with all the requirements of the Privacy law, particularly those concerning notification when collecting information. It is however arguable that failure to meet the highest standards of notification in a case like KIWI PRODUCTS, where the intended uses are reasonably self-evident and the risk of harm is low, does not undermine individuals' rights in a significant way. The important fact is that KIWI PRODUCTS is liable under the Privacy Act for breaches of any of the privacy principles and that comprehensive and easily accessible remedies are available for anyone, including overseas customers, for breaches of most of the principles (although not in relation to access and correction).

Data in Electronic Commerce

(f) *United States of America*

The Nature and Circumstances of the Transfer

1. USDM is a company with headquarters in the State of Ohio that sells consumer items (primarily clothing) through a mail-order catalogue. The company was founded within the last twenty years as a small-scale operation, and it remains family owned. Individual entrepreneurs began many American direct marketing and information companies in a similar manner. The company supports its sales and other customer services through a toll-free 800 number and through fax lines, and it has a special telephone number for overseas callers as well. The company now also operates retail stores in several states. Most sales are to North American consumers, but an increasing number of USDM customers can be found elsewhere around the world.

2. The description presented here is representative of an average American direct marketer that maintains a website in addition to its other operations. USDM recently established a website that permits consumers from any country to place orders for products over the Internet. Sales over the Internet are small, but significant growth can be anticipated as commerce on the Internet expands. At company headquarters in Ohio, USDM collects and maintains information about consumers placing orders through the website.

3. As is typical of many American direct marketers, USDM rents its list of customers through a list broker. The rental process allows the company to review how a proposed renter proposes to use the list. In practice, it is unusual for a prospective list renter to be denied the list, although it does happen occasionally. The company does not yet rent the mailing addresses of its international customers, although it is considering doing so in the future. The customer list that is currently rented can be segmented by gender, recency of order, amount and frequency of purchase, and geographic location. The use of nine-digit postal codes permits additional identification of consumers by demographic characteristics common to small geographical areas. The segmentation done by USDM is customary throughout the direct mail industry.

4. Standard list-rental practices include removal of duplicate names and addresses that appear on other lists being used, removal of names and addresses from an industry-run ‘do not mail’ list, standardising address formats to meet postal requirements, and the addition of ‘dummy’ names to the list. The dummy names enable the list broker to monitor use of the list to make sure that it has only been used for an approved purpose and for the authorised number of times. The company collects e-mail addresses of web-page visitors, but it does not currently sell, rent, or otherwise share them.

5. USDM is a member of the Direct Marketing Association (DMA), the principal trade association for American direct marketing companies. USDM is also a member of the Better Business Bureau (BBB) and a few other industry associations.

6. USDM’s attention to privacy issues is better than many other companies, although a few other companies have more detailed and more complete privacy policies. Many companies selling goods and services on the Internet do not have any privacy policies and do not belong to the DMA or other relevant trade associations.

Overview of the Regulatory Environment for This Case

7. No federal or state data protection statute applies to the activities of USDM. No federal or state agency has responsibility for comprehensive oversight or enforcement of direct marketing or electronic commerce data protection activities.

8. The Federal Trade Commission (FTC), an independent regulatory agency in the United States Government, has some authority to enforce privacy policies through its jurisdiction over unfair trade practices. The FTC's authority was never used in a privacy case until August 1998, when the FTC brought a complaint against a website that had a misleading privacy policy that did not reflect the company's actual practices. In theory, other FTC actions could seek to enforce compliance with privacy standards. The FTC has been active on privacy matters in recent years, but it is unlikely that the agency will issue formal privacy rules that would be binding on American companies. Also, the FTC's ability to bring privacy actions against companies that do not have privacy policies is in doubt. The first case was brought against a company that did not comply with its own stated policy. Future privacy enforcement actions are possible, but it is unlikely that the FTC will be anxious to investigate individual consumer complaints. Nevertheless, the FTC is currently a looming presence for American companies operating websites.

Purpose Limitation, Transparency and Opposition

9. Customers who order through the USDM website provide their name, address, telephone number, e-mail address, and credit-card number. The company maintains all this information along with the purchasing history for its customers. These are standard practices for direct marketing companies.

10. The USDM website tries to set a cookie (client side persistent data) at times during the order process. The website does not function as planned unless the customer accepts the cookie. For example, the only way that the website can track the order of more than one item being purchased is through a cookie. The use of cookies during online ordering is a standard industry practice. The cookie set by USDM is temporary, and it expires in approximately 24 hours.

11. No general federal or state data protection statute expressly regulates the collection, use, or disclosure of personal information obtained through marketing. The federal Video Privacy Protection Act regulates the disclosure of information about the sale or rental of videos, but USDM is not engaged in that business. Video sale and rental records are one of the few classes of marketing information regulated by federal or state statute.

12. In the absence of federal and state laws, the only source of limitations on collection, use, and disclosure practices is company and industry practice. The company appears to collect from its customers only the information that is needed to fulfil orders. Neither the company's printed catalogue nor its website displays a common statement of information practices that describes how personal information from customers is collected, maintained, used, and disclosed.

13. The website does include a modestly descriptive privacy policy that details some collection practices. For example, the company discloses that it does not collect e-mail addresses of website visitors. It only collects the domain name. For those who communicate through e-mail, however, the company records any information provided by the consumer, including name, address, and e-mail address. The company expressly tells customers that it does not sell, rent, or share e-mail addresses. The company discloses that it will send catalogues to any consumer who provides a mailing address. The company may call a customer who has provided a telephone number to inquire about an order that was placed, but it does not share telephone numbers with other organisations. It does not offer an express 'do-not-call' option, but a consumer can decline to provide a telephone number. Once the number has been provided, however, there is no clear method to tell the company not to call. Presumably, the company would honour a request received by telephone, mail, or e-mail.

14. The company will remove a name from its mailing list. It provides an e-mail address, toll-free telephone number, and mailing address for consumers to contact for this purpose. In addition, the company maintains it own 'do-not-rent' list that allows a consumer to remain on the USDM mailing list without having his or her name rented to others.

15. The website privacy notice offers more information than does the company's catalogue. The catalogue offers separate choices allowing a consumer to be removed from the USDM mailing list or to keep his or her name from being shared with others. The catalogue includes a description of the DMA's Mail Preference Service (MPS). This service allows consumers to have their names removed from multiple industry mailing lists. The catalogue provides a postal mailing address for the MPS, but no e-mail address. The website does not mention the MPS anywhere. The MPS does not currently accept addresses of consumers outside the United States. Some American companies that mail internationally use the mail preference lists maintained by marketing associations in other countries. The DMA does not require that its members use international mail preference lists, although some international mailers may use one or more mail-preference lists from European Union member states.

16. For both catalogue and website, the opt-out procedures are clearly explained and relatively simple for consumers to use. The catalogue order forms includes tick boxes for a consumer to express a choice. This is not a universal practice. Not all American companies currently offer an opt-out to consumers. Some offer an opt-out, but the information is not as prominently displayed as is the case with USDM. Some companies that offer an opt-out require consumers to send a letter separately from an order and to a different address. USDM's opt-out is clear, visible, and easy to use.

17. USDM's website appears to comply with the marketing industry standard for consumer choice. DMA's currently optional guidelines advise marketers who collect information online from consumers and who share that personal information with other companies to allow consumers the ability to prohibit the disclosure of such information. USDM offers an opt-out to consumers in a clear manner. It does not offer an affirmative choice (opt-in) to be on a company list, and the DMA does not ask its members to use an opt-in.

18. DMA's current guidelines also tell marketers that they should provide consumers with a prominent notice of information practices. The DMA's notice guidelines do not describe the appropriate level of detail for the disclosure notice. USDM has an online privacy policy statement that appears to serve as a general notice of information practices. However, the printed catalogue does not have an identifiable notice of privacy practice or of information practices. Compliance with DMA privacy standards is not currently a requirement for membership in the association, but the DMA has announced that notice and opt-out rules will become mandatory in July 1999. The specific details of the new requirements have not been announced.

19. It is possible that the company's customer list could be requested or subpoenaed by a federal, state, or local law enforcement agency. It is difficult to imagine circumstances in which an entire customer list from a reputable company like USDM would be needed. It is foreseeable that individual records could be useful in investigations of credit-card fraud. Government access to marketing lists of the type maintained by USDM does not appear to be common. However, federal agencies have from time to time rented marketing lists for use in law enforcement investigations. The practice of renting lists to federal law enforcement agencies has been controversial within the industry, but the sale of lists proceeded anyway because it was not possible to prevent all participants from refusing government requests. Nothing in the USDM online privacy notice discusses the possibility of disclosure to governmental agencies, but USDM lists have not been rented to government agencies.

Data Quality and Proportionality

20. USDM's data collection activities are defined directly by its need to fulfil an order from a customer. The company needs to be able to contact its customer by postal mail and sometimes by e-mail or by telephone. The information collected appears to be typical of others who are engaged in the same type of business. There are no externally imposed limits for the accuracy, relevance, timeliness, or completeness of personal data held by marketing companies

Security

21. USDM recognises that its database is a corporate asset, and it has taken steps to protect the value of that asset from outsiders. Standard computer security tools are used, including password protection. However, more specialised privacy protections for consumer information are mostly absent. Controls over access and use by employees have not been implemented, and those who can use the database can see any consumer information, including credit-card data. No audit trails are maintained. The company does not offer privacy or security training to employees and does not have any formal policy statements for employees on security or customer privacy.

22. Consumers placing orders over the Internet can use standard browser security tools. The website encrypts order and credit-card data using Secure Socket Layer (SSL) encryption. A security notice on the website informs customers how the SSL security feature is activated during the ordering process.

Access and Rectification

23. No federal or state law requires a marketing company like USDM to give individuals access to the personal information in its files. Similarly, the DMA privacy guidelines are silent on access. Given the limited information maintained on customers, there is no reason why USDM would refuse to correct an inaccurate record. The company takes steps to keep its address list current by using information on changes of address provided through services authorised by the United States Postal Service.

24. While the DMA privacy guidelines are silent on access and rectification, another industry trade association has taken a slightly more positive position. The Online Privacy Alliance is a new coalition of companies and trade associations (founded in 1998) that has a common goal of satisfying consumer expectations for privacy in the online environment. Self-regulatory privacy principles adopted by the Alliance address data quality and access. The principles require member organisations to take reasonable steps to assure that data are accurate, complete, and timely for the purposes for which they are to be used. Organisations are expected to establish appropriate mechanisms for correction of inaccuracies in 'material individually identifiable information'. These mechanisms may include consumer access and correction. A careful reading of the guidelines makes it clear that no member of the Alliance is required to provide direct consumer access and correction rights. The issues of access and correction have been highly controversial among portions of the American business community, and many companies are adamant in refusing to agree to mandatory access and correction. The DMA is a member of the Online Privacy Alliance. While DMA privacy guidelines will soon become mandatory for DMA members, it does not appear that the requirements of the Alliance will be mandatory on DMA members as well. USDM is not a member of the Online Privacy Alliance.

Onward Transfer Restrictions

25. At present, USDM does not transfer consumer information to other jurisdictions. Its list of international customers is not currently available for rent. Even if it were, the transfer of the list would be under standard controlled conditions designed to make sure that the list is use only for the purpose for which it was rented. Because of the corporate need to protect its customer list asset against unauthorised use, it is reasonable to expect that the company will take appropriate steps to control use of its list. Nevertheless, a transfer of the list to another jurisdiction could happen if the company chose. No federal or state law would prevent the transfer of the company's customer list to another jurisdiction.

Remedies

26. In the United States, statutory remedies for consumers aggrieved about violations of fair information practices by direct marketers are rare. No specific statutory remedies under Ohio law appear to be available against USDM. Common law tort actions may theoretically provide the possibility of a remedy for some privacy breaches. Ohio tort law recognises the privacy torts of unwarranted appropriation of personality, publicising of private affairs of no legitimate public concern, and wrongful intrusion into private activities in such a manner as to outrage or cause shame or humiliation. Whether any of these tort actions would result in enforcement of fair information practice principles is problematic. There appear to be no precedents of privacy actions being brought against marketers in Ohio. Breach-of-contract actions might be possible against USDM for a direct violation of a stated privacy policy. Ohio consumer protection laws might arguably provide the basis for some consumer relief, but no relevant precedents are available.

27. In direct marketing relationships, information typically flows from the consumer to the marketer and not through an intermediary. That is the case with European customers doing business with USDM. No European data controller or processor will be involved in the transaction. This means that any remedy for the consumer will have to come directly from the American company. The European consumer will have to find and use one of the remedies available in the United States or provided by the company. The alternatives currently available are not easy to use or inexpensive. They do not offer the promise of significant relief, and USDM does not offer an independent privacy dispute resolution mechanism. As a result, it is difficult to conclude that the remedies currently in place offer much protection to European consumers.

Accountability

28. The marketing industry offers several accountability mechanisms with limited utility for consumers. The DMA's Committee on Ethical Business Practice accepts and considers complaints about data collection and list rental practices, as well as other issues of compliance with DMA policies. The Committee is composed solely of members of the DMA, and little information on is available on its activities. DMA publishes an abbreviated summary of Committee actions. It appears that the Committee will accept consumer complaints, but the Committee has not authority to award damages. The Committee may nevertheless help consumers to pursue complaints against members, although the availability of the Committee's services is not publicised to consumers. Members are not currently required to comply with decisions by the Committee, although this could change when the association adopts mandatory new privacy policies in July 1999. It appears that the Committee is successful some of the time in persuading companies to comply with DMA guidelines.

29. The DMA also offers its members a printed fair information practices checklist that a company can use to assess its own privacy policies and practices. Use of the checklist is not mandatory, and USDM has not applied the checklist to its operations. The DMA also

assists members in establishing privacy policies through a website privacy policy generator. USDM has an Internet privacy policy that it developed on its own.

30. The Online Privacy Alliance adopted a set of self-regulatory enforcement policies. The Alliance believes that effective enforcement of self-regulation requires verification and monitoring; complaint resolution; and education and outreach. Several methods of third-party verification of compliance with privacy policies are in place or in development in the United States. USDM is not a member of the Alliance or any of the third party verification organisations, such as TrustE. Some third-party verification programmes offer the use of privacy 'seals' that can be displayed on websites to assure consumers that privacy rules are in place and that remedies are available. Whether these seal programmes will be successful remains to be seen.

31. Consumer complaint and enforcement mechanisms are also in development in the United States. The BBB Online programme is developing a dispute resolution mechanism for privacy that may parallel its dispute-resolution mechanism for other consumer disputes. It is too early to assess the scope of the programme. However, it is already clear that the awarding of monetary damages to aggrieved consumers will not be readily embraced by American businesses. USDM has not agreed to support the announced, but not yet operational, BBB Online dispute resolution programme.

Conclusions

32. Complete fair information practice protections including enforcement for consumers who are the subject of marketing data in the United States are rare. This conclusion is the same for online and offline activities. Marketing is, for the most part, an unregulated activity so no external fair information practice requirements exist.

33. At present, industry self-regulatory practices offer the best chance for compliance with fair information practices. However, current voluntary privacy guidelines of the DMA offer consumers only notice and opt-out. The remaining elements of fair information practices are not addressed by the DMA guidelines. Even when those guidelines become mandatory in July 1999, it is not clear that any additional elements will be included, with the possible exception of an internal DMA enforcement mechanism that may offer a limited remedy for consumers. The Online Privacy Alliance self-regulatory guidelines address additional fair information practice elements, but how those guidelines will be applied by companies remains to be seen. The Alliance offers the prospect of more comprehensive enforcement and accountability mechanisms than does the DMA, but those mechanisms are still in development.

34. In summary, even for companies like USDM that generally comply with industry standards and legal requirements, the fair information practice protection for consumers are substantially incomplete. Industry codes do not address all fair information practice elements. Limited help is available to consumers with privacy complaints, and formal mechanisms for relief are rare.

Conclusions about Data in Electronic Commerce

1. Compliance with fair information practices for the six electronic commerce transfers studied is almost wholly dependent on whether the jurisdiction has a comprehensive data protection law. In Hong Kong and in New Zealand, private-sector data protection laws require companies to comply with a range of requirements that generally meet the standards set out in the European Union Data Protection Directive. A similar law exists in the Canadian province of Quebec.

2. In other jurisdictions, no law applies general fair information practices to electronic commerce activities. As a result, electronic commerce is virtually unregulated for data protection. The nature of most electronic commerce activities makes it unlikely that good practices by EU organisations will be exported to their foreign counterparts. In many instances, the relationship between an EU customer and a foreign company will be direct and without any intermediary.

3. Voluntary industry codes exist in the jurisdictions without applicable laws, but the extent to which those codes address fair information practices, let alone meet the standards in the EU Directive, is highly variable. Even where codes exist, many companies are not members of the trade associations that have promulgated them. Also, electronic commerce involves a wide range of activities, and existing trade associations - like direct marketing associations - will not necessarily encompass all participants within their membership. Codes may vary from industry to industry as well. The international nature of consumer electronic commerce activities also presents a challenge to voluntary codes, which tend to be national and not internationally based.

4. The availability of an independent complaint mechanism is also tied to the presence of a general data protection law. In other jurisdictions, voluntary mechanisms might be available through trade associations or otherwise, but consumers are not likely to find completely independent dispute-resolution mechanisms.

5. A customer may be able to determine the extent to which a foreign company addresses fair information practices if an on-screen notice is available. However, many websites do not include privacy notices, and many existing notices do not address all elements of fair information practices.

Sub-contracted Data Processing

(a) *Australia*

The Nature and Circumstances of the Transfer

1. The OUTSOURCING CORPORATION OF AUSTRALIA (OCA) is a large multinational company that provides a complete range of information technology services to a large and diverse range of public and private client organisations. These services include traditional bureau processing, as well as more advanced data warehousing, applications maintenance and network management, all of which will typically involve the handling of customer personal information.

2. All data processing by OCA on behalf of clients is strictly controlled by contract. As a general matter, data processing contracts do not distinguish between personal and non-personal data. If the data are controlled by a client, than the processor has strict obligations for confidentiality. Non-disclosure rules will be designed largely to protect the corporate interest of the client. It is typical practice in the outsourcing industry for such contracts to be shrouded in considerable secrecy, and all guidance about processing is determined by the client through the contract with OCA. It has therefore been impossible to establish what personal data are processed by OCA in Australia, and on what precise terms and conditions (There has incidentally been a major public debate in Australia about the alleged loss of public accountability resulting from contracting out of government services to the private sector. The secrecy surrounding the terms of such contracts has been particularly criticised).

3. The type of data processed might be any type of personal record routinely processed by computer, such as those relating to telephone bills, credit transactions, health insurance claims, cable television subscriptions, or government taxes or benefits. For the purposes of this case study, WATELEC is a major utility company (a publicly listed company but partly government owned), operating in several European Union (EU) countries, which contracts with OCA to process its entire customer database in Australia, with daily batch transfers to and from the source countries. The contract between WATELEC and OCA stipulates that ownership and control of any data processed under the contract (not just any transferred from WATELEC, but also any collected or generated by OCA) remains with WATELEC. OCA are constrained to only collect, process, use and disclose data as expressly authorised by WATELEC or as necessary to perform contractual obligations.

Overview of the Regulatory Environment for This Case

4. There is currently no privacy law in any Australian jurisdiction that applies to the activities of a data processing contractor such as OCA. Neither the federal (Commonwealth) Privacy Act 1988 nor the Telecommunications Act 1997 (which contains some privacy provisions implemented through a complex system of co-regulatory codes), apply to such an activity. However, a Bill to amend the Privacy Act to apply it to contractors providing services to the federal government was introduced in the first half of 1998 and in September was still before the Senate when a federal election was called. This Bill, if enacted in the new Parliament, would make a contractor such as OCA subject to the Information Privacy Principles and the full enforcement mechanisms of the Act, but only in respect of personal information it was handling for or on behalf of a federal agency.

5. At least since the Privacy Act commenced in 1989, some federal government agencies have been including privacy protection clauses in contracts with service providers, particularly in major contracts for IT services and data processing. The Privacy Commissioner issued guidelines and model clauses in 1994 and the Department of Administrative Services included this advice in its own contracting guidelines.

6. Following the federal government's rejection of a statutory privacy protection in March 1997, the Privacy Commissioner has been developing National Principles for the Fair Handling of Personal Information (NPs). A first set of Principles was issued by the Commissioner in February 1998 following intensive consultation with business, government and consumer representatives. They have been drafted with the EU Directive very much in mind, and were regarded by the Commissioner as being international 'best practice'. In light of further comments, and the prospect of the Victorian government legislating the principles (see below), the Commissioner commenced further consultations in August 1998 to review some aspects of the National Principles.

7. The Victorian government has announced that it proposes to legislate for privacy protection in both the public and private sectors in the State, and in July 1998 released a discussion paper setting out its plans. It proposes to enact the Privacy Commissioner's National Principles as the default standard, but to allow for sectoral or activity codes of practice, developed through a consultative process and approved by a Privacy Commissioner, to replace the default Principles. It remains unclear whether the compliance and enforcement mechanisms of the new law would apply equally to the default statutory principles and to any approved codes.

8. The Australian Information Industries Association (AIIA) has been involved in the Privacy Commissioner's consultation process, and is expected to commence the development of a code of practice to give effect to the National Principles. OCA is a member of AIIA, and will presumably be bound by any privacy code that the Association develops.

Purpose Limitation, Transparency and Opposition

Collection

9. In relation to the collection of customer information, it is assumed that WATELEC complies with the data protection law of the various European countries in which it operates. The service provided by OCA involves some data about customers being provided directly to OCA by third parties in Europe, such as financial institutions processing direct debit payments, but these again will be subject to the relevant European law. OCA need not take any independent steps to meet fair collection or notification requirements of collection principles, or to obtain the consent required for the collection of any 'sensitive' classes of personal data under Article 8 of the EU Directive.

Use and disclosure by OCA in connection with the contract

10. The processing involved in the performance of the contract is quite complex and includes a variety of matching routines, as well as profiling to generate targeted personalised marketing communications. Customer master records are routinely updated with water-consumption data provided by WATELEC and billing information generated and transferred directly to other contractors in Europe for printing and mailing. Again, all of these operations are performed on behalf of WATELEC under detailed instructions contained in schedules to the contract.

11. The contract specifies that control of any data, including personal information, held by OCA in connection with the contract remains with WATELEC. Any independent use of the information by OCA would be a breach of contract, but would not be unlawful under any Australian statute.

Disclosure to third parties for their purposes

12. The 'output' data include a variety of returns to government agencies in the source countries; these are transferred by OCA to WATELEC rather than provided directly.

13. It is difficult to envisage why a government authority in Australia would seek access to information about WATELEC customers held by OCA, but the possibility exists - perhaps as incidental evidence in relation to investigations about OCA's compliance with Australian laws. For disclosures to third parties in Australia for a purpose of a third party, OCA is required by contract to obtain WATELEC's express consent, except that the contract allows them to disclose information in an emergency situation where there is a imminent risk to life or health of any person, provided they notify WATELEC after the event. In all other circumstances, even if there were a legal requirement to disclose within Australia, OCA would refer requests to WATELEC's legal department. The same would apply to any requests from European authorities, although these would normally be expected to come through WATELEC in the first place.

Data Quality and Proportionality

14. Regardless of the type of personal data processed under a sub-contract, it is difficult to expect a sub-contractor independently to apply quality standards, other than to ensure data integrity through precautions against inadvertent corruption of the data. Other quality control policies must originate with and be applied directly by the data controller, WATELEC.

15. OCA is required by the contract to apply a data-retention policy that includes destruction of data after a specified period of time, or in some cases, the return of data to WATELEC for archival storage.

Security

16. One area where it is possible to assume that a sub-contract imposes detailed data protection requirements is security. Clients usually have good reasons for protecting their data other than privacy requirements, so it is not surprising that security is a routine feature. Confidentiality requirements are common in data-processing contracts, but details vary widely from contract to contract.

17. While OCA can be expected to offer a fairly high 'base' level of security, additional measures and precautions are likely to be optional, available for a charge, and will depend in this case on what WATELEC is willing to purchase. Options may include varying levels of backup, disaster recovery, a dedicated security officer, written security requirements, audits, access controls and monitoring, audit trails, and encryption. A large processing company like OCA should be able to provide a great deal of security. Unlike some countries, there are currently no government restrictions in Australia on the level of encryption that can be applied.

Access and Rectification

18. The contract between WATELEC and OCA would not make any express provision for 'subject' access or correction requests. WATELEC's customers could be expected to approach the company directly if seeking access. OCA would, on instruction, carry out to meet WATELEC's requirements for satisfying the relevant European law. If an individual approached OCA directly, then OCA would deal with the request in the same way as any

request for disclosure - by referring it to WATELEC in accordance with the terms of the contract.

Onward Transfer Restrictions

19. There is nothing in Australian law to prevent OCA from transferring the data its processes on behalf of WATELEC to a third country, but if it did so outside the terms of its contract with WATELEC it would lay itself open to a breach of contract action. Outsourcing contracts normally contain a requirement for the prime contractor to obtain the client's express approval for any sub-contracting.

Remedies

20. Express consumer remedies have in the past rarely been included in data processing contracts, although OCA in Australia would have some experience of privacy protection clauses in contracts with government agencies. These have included a requirement for the contractor to co-operate with any investigation into an alleged breach of privacy, and to notify the client of any consumer complaint.

21. Unlike in some other jurisdictions, Australian law does not recognise any interest by a third party in a contract. If the contract between OCA and WATELEC were under the law of any Australian State or Territory, it would not be possible for an aggrieved data subject to use the contract between the data controller and the processor as a basis for a lawsuit against the processor. This may be an option if the contract was under the law of a European country where the legal system gives third parties these rights.

22. Even if a lawsuit were legally supportable, many barriers remain. First, the contract must contain clauses that were intended to benefit a data subject. If the contract is silent about privacy requirements or unclear about the intended benefits to a data subject, then the lawsuit may fail. For example, contractual security requirements intended to protect a controller’s interest in the confidentiality of its data may not create a cause of action by the data subject. The data subject may be an incidental beneficiary with no basis for a lawsuit because the protection of the subject’s privacy was not the main purpose of the security requirement. Second, lawsuits are cumbersome and expensive. Foreign nationals might find it to be especially burdensome to sue an Australian company in an Australian court. Third, proving damages in privacy actions is often challenging. Unless a substantial monetary recovery is possible, attracting a lawyer willing to file a lawsuit can be difficult.

23. Even if the OCA/WATELEC contract could not be enforced directly by an individual, it could in theory contain the same rigorous terms as were required by the German Data Protection Commissioner in the 1995 contract between German National Railways and Citibank in the United States, referred to in the Article 29 Working Party's Working Paper No 9. This provided, for instance, for an individual German complainant to deal throughout the course of a complaint with the German Commissioner and the client organisation, even though the action complained about may have been by the contractor and have taken place in the United States. But as the Working Party points out, there are many practical difficulties in ensuring that contractual provisions do in fact provide individuals with easily enforceable remedies.

Accountability

24. WATELEC is subject to accountability requirements in its home country. In the absence of any law or relevant code of practice in Australia, the contract between OCA and WATELEC is likely to be the only source of any accountability measures in relation to the

transferred data. The contract could include provision for such things as OCA's reporting to WATELEC about its compliance with and data processing terms in the contract, about auditing, about staff training for privacy protection, etc.

Conclusions

25. It is impossible to offer any general conclusions about adequacy of data protection when an Australian company processes data on behalf of an EU-based data controller. For the most part, Australian statutory and common law impose few requirements on data processors and offer no assistance to data subjects. Even where laws exist, they are likely not to be applicable to data that are processed in Australia on behalf of an overseas client. The scope and degree of processing may make a difference in some instances, however. If an Australian contractor performs enough substantive processing activity, it is possible that the activity will fall under the limited Australian privacy laws or self-regulatory guidelines in some cases. In the end, however, privacy protection in Australian laws remain a patchwork quilt, applying only to limited sectors or narrow classes of data. The services provided by OCA for WATELEC in this scenario are not subject to any statutory controls.

26. The only other source of privacy protections is the contract between controller and processor. Because it has proved impossible to obtain direct access to these contracts in the course of this project, no general conclusions about the scope or content of these contracts can be offered. The limited amount of information available suggests that while there will be some strict security and confidentiality and data integrity provisions in major data processing contracts, they will not meet all of the criteria suggested by the Article 29 Working Party as necessary to provide 'adequate' privacy protection.

Sub-contracted Data Processing

(b) *Canada*

The Nature and Circumstances of the Transfer

1. The GLOBAL PROCESSING CORPORATION (GPC) is a large multinational company that provides a complete range of information technology services to a large and diverse range of public and private client organisations. The services range from the deployment of hardware and software, to user training, to network management, to infrastructure development, to more traditional data management and processing functions. It has thousands of clients in virtually every economic sector in over 40 countries around the world.

2. All data processing by GPC on behalf of clients is strictly controlled by contract. As a general matter, contracts do not make a distinction between personal and non-personal data. If the data are controlled by a client, than as the processor, GPC has strict obligations for confidentiality and non-disclosure. It is typical practice in the data processing industry for such contracts to be shrouded in considerable secrecy. It has therefore been impossible to establish what personal data are processed by GPC in Canada, and on what precise terms and conditions.

3. The present discussion does not assume a specific scenario involving the sub-contracted processing in Canada of a particular type of personal data originating from data controllers in countries of the European Union (EU). The type of data processed by a sub-contractor could be any type of personal record routinely processed by computer, including telephone billing, credit transaction, medical records, cable television subscriber information, other kinds of personal consumer data, school records, governmental tax, or virtually any other record. For the purposes of this case study, we assume that the processing is taking place in New Brunswick, a Province that has actively been trying to encourage high-tech industry in recent years.

Overview of the Regulatory Environment for This Case

4. GPC (Canada) is not subject to any general data protection legislation in New Brunswick. No Privacy Commissioner exists in that Province, although complaints can be registered with the provincial Ombudsman for privacy abuses in the public sector. At the federal level, neither the Privacy Act, nor the Telecommunications Act, which contains a brief privacy provision overseen by the Canadian Radio and Telecommunications Commission (CRTC), apply to activities such as these.

5. For purposes of analysis for the Canadian case, we assume that GPC (Canada) has registered to the ISO 9001 quality assurance standard, and is currently developing procedures to bridge or link to the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information (Q830)[8] to that standard. The Registrar is the Quality Management Institute (QMI) of the CSA, which is the only accredited Registrar in Canada to have offered explicit registration services to the privacy standard.

6. No Canadian business has yet to register to Q830, but several organisations, including some in the data processing industry, are actively contemplating such a registration as a result of pressure from federal and provincial governments and Privacy Commissioners. An increasing number of media stories have been critical of the data

[8] Canadian Standards Association, Model Code for the Protection of Personal Information, Q830 (Rexdale, Ontario: CSA, 1995)

processing industry in Canada and sceptical of the protections afforded to personal data once they are handed over by government for processing.

7. A variety of incentives might encourage organisations involved in sub-contracted data processing to adopt the CSA standard. Some might have a desire to avoid adverse publicity. Others might believe that there is a competitive advantage to being able to demonstrate compliance to privacy standards and thus gain a 'good housekeeping seal of approval'. But more coercive inducements might also operate. Unlike a code of practice, a standard can be referenced in contract either between private enterprises or between government and a private contractor. For instance, if a private contractor processed personal data under government contract, a simple way for the government agency to ensure the adherence to the same data protection standards as apply in government would be to require the contractor to register to the CSA Model Code. The same could apply to international contracts and the transborder flow of data.

8. It is not, therefore, unreasonable to assume that a company like GPC (Canada) might see considerable benefits in registering to Q830. QMI will register a company to the privacy standard alone. But it also offers a process that couples the requirements of an ISO 9000 quality system registration with the requirements of the Q830 privacy code. For the purposes of this analysis, we assume that GPC (Canada) has been registered to the ISO 9001 quality management system for a number of years. For the purposes of this case, adequate data protection within GPC (Canada) is, therefore, measured principally against the content of Q830, as well as the process by which the company translates those principles into practice.

9. Registration to any standard is based on the simple adage, 'say what you do and do what you say'. GPC (Canada)'s first task is therefore to define the scope of its operations to which Q830 will apply. For the purposes of the initial registration, it concludes that it will first apply the standard to those personal data collected as a result of sub-contracting with public and private organisations. It decides to leave aside, for the time being, the question of the protection of the personal information of its employees. GPC (Canada) determines that, while it is not the original collector of personal information, the CSA standard does indeed apply. 'Collection' is defined as: 'the act of gathering, acquiring, or obtaining personal information form any source, including third parties, by any means.'

10. Having defined the scope of application, GPC (Canada) is then expected to develop a code of practice. This should contain all ten principles within the CSA Model Code, together with some commentary that explains how the organisation implements each principle in practice, providing specific examples. The code is described as a 'voluntary' standard. However, should an organisation choose to adopt the principles and practices contained in the standard, 'the clauses containing prescriptive language become requirements'.

Purpose Limitation, Transparency and Opposition

Collection

11. Principle 2 of the CSA Model Code declares that 'the purposes for which personal information is collected shall be identified by the organisation at or before the time the information is collected.' The CSA Model Code is based on a requirement of transparency. In many ways the accurate identification of the purposes for which information is collected is the basis for the entire CSA Privacy Code. Under the CSA standard, OCA would be considered to have 'collected' personal data, defined as 'the act of gathering, acquiring, or obtaining personal information from any source including third parties, by any means.'

12. In implementing this provision, GPC (Canada)'s Privacy Code of Practice states the purpose of collection, related to each category of individuals on whom data are collected. The documentation of purposes should be readily available (and ideally presented in the GPC Privacy Code) and be easily and clearly understood.

13. Most of this provision, however, is less relevant for GPC than it is for the controller. The statement of purposes would likely be very broadly described. The contract would specify that control of any data, including personal information, held by OCA in connection with the contract remains under the control of the client/controller. Any independent use of the information by OCA would be a breach of contract. This relationship would need to be explained in full in the GPC Privacy Code.

Uses and Disclosure for GPC Purposes, or to Third Parties for Other Purposes

14. The standard makes no normative distinction between internal use and external disclosure. Principle 5 applies in either case: 'Personal information shall not be used or disclosed for purposes other than those for which it as collected, except with the consent of the individual or as required by law.'

15. Principle 3 says that 'the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.' The principle also requires 'knowledge and consent'. Thus, consent is inextricably connected with the implementation of Principle 2, and transparency can be accomplished through the clearly defined communication of purposes. There are only very limited conditions under which the obtaining of consent would not be appropriate. These situations include cases of law enforcement investigations; cases of medical emergency or mental incapacitation; and cases where the organisation does not have a direct relationship with the individual concerned. This last exception applies to GPC (Canada), because it is the processor rather than the controller of the personal data. GPC (Canada) explains this exemption in its code, and commits itself to avoid any further secondary uses beyond those that are immediately defined in the contract with the controller.

16. In the circumstances where GPC (Canada) is approached by a government authority for access to the client's data, prior to the disclosure they are obliged to notify the client of the request, affording the client the right to challenge the access. A contractual provision might read: 'If confidential information is required to be disclosed pursuant to a requirement of a governmental authority, such confidential information may be disclosed pursuant to such requirement so long as the Party required to disclose the confidential information, to the extent possible, provides the other Party with timely prior notice of such requirement and co-ordinates with such other Party in an effort to limit the nature and scope of such required disclosure.' These practices are also outlined in the GPC Privacy Code.

Data Quality and Proportionality

17. Principle 4 of the CSA Model Code deals with the limitation on collection: 'The collection of personal information shall be limited to that which is necessary for the purposes identified by the organisation. Information shall be collected by fair and lawful means.' This principle does of course entail a review of information management to ensure that irrelevant, obsolete, or incomplete information is not collected. Principle 5 also states that 'personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.'

18. Organisations are also therefore obliged to develop guidelines and to implement procedures with respect to the retention of personal information. Ideally these guidelines should include minimum and maximum retention periods. Information that is no longer

required to fulfil the identified purposes should be 'destroyed, erased, or made anonymous'. A minimum retention policy should be developed for all categories of personal data collected by GPC (Canada). This will be included in the contract with the client. A contractual provision might read: 'Upon written request at the expiration or termination of this Agreement for any reason, all such documented confidential information (and all copies thereof) owned by the requesting Party will be returned to the requesting Party or will be destroyed, with written certification thereof being given to the requesting Party. The provisions of this Section will survive the expiration or termination of this Agreement for any reason.'

19. Principle 6 states: 'Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.' GPC (Canada) describes in its code of practice the processes used to clean certain data received under contract.

Security

20. The safeguards principle (Principle 8) of the Model Code is perhaps the most important for GPC (Canada): 'Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.' This means that a range of physical, organisational and technological measures may be appropriate given the sensitivity of the data collected by the company. Organisations are also expected to remind employees constantly of the importance of maintaining the confidentiality of such information. All such safeguards and measures should be openly stated.

21. As a general matter, client contracts include security requirements. The applicable contractual commitments are communicated to the employees responsible for their implementation. Contracts also stipulate clear procedures for audits in terms of their scope and procedures. Access controls are routinely used to identify wrongful access or attempts to access data. With its mainframe applications, GPC (Canada) also implements audit trails to record both internal and external access. Whether encryption is used depends on the specific requirements and the contractual provisions. All physical, technological and organisational security measures are described in GPC (Canada)'s Privacy Code.

Access and Rectification

22. Principle 9 of the CSA Model Code stipulates: 'Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.' As the processor of the personal data, GPC (Canada) passes any requests for subject access and correction to the client/controller of the data.

Onward Transfer Restrictions

23. Principle 4.1.3 of the CSA Code stipulates that 'an organisation is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organisation should use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.' The expectation is that the CSA privacy standard could be the mechanism by which contractual obligations are passed on. Thus, if GPC (Canada) used a sub-contractor to process some of the personal data for some clients, it would be responsible for ensuring that the sub-contractor would also conform to the privacy standard.

24. A client contract may also stipulate procedures or limitations respecting the location of processing. In some cases local laws may be a consideration, restricting or prohibiting

certain transfers. These laws would frequently not be premised upon privacy principles, but rather principles of national security (e.g., military classified information) or political considerations (e.g., taxpayer information). The realities of the data processing transaction dictates that the client-controller of the data maintains control of the data and any uses to which it is put. Frequently GPC (Canada) is allowed a degree of latitude in determining specifics of the processing, but it never exercises control over the uses of the client's data. But there is nothing in Canadian (or New Brunswick) law to prevent OCA from transferring the data its processes to a third country, but if it did so outside the terms of its contract with the client/controller it would lay itself open to a breach of contract action.

Remedies

25. Under Principle 8 (openness), GPC (Canada) is also expected to 'make readily available to individuals specific information about its policies and practices relating to the management of personal information.' This information may include the name and address of the designated individual; the means of gaining access to personal information; a description of the type of personal information held by the organisation; a copy of any materials that explain the organisation's policies and practices; and what personal information is available to related organisations (e.g., subsidiaries).

26. Under Principle 10, 'an individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.' GPC (Canada) is expected to put procedures in place to receive and respond to complaints relating to their handling of personal information, and to take appropriate measures if a complaint is found to be justified. It is also expected to inform individuals (through its code) of the existence of other relevant complaint mechanisms, a range of which might exist. GPC commits itself (in its Code) to abide by the judgement of an external arbitrator if an individual's complaint is not satisfactorily resolved at the company level.

Accountability

26. How, then, does GPC (Canada) ensure that it 'does what it says'? Several mechanisms are provided through the CSA Code registration process.

27. First, Principle 1 of the CSA Code states that 'an organisation is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organisation's compliance with the following principles.' This may seem obvious, but it is significant that this principle is placed first. The designation of one person, whose duties may of course include other responsibilities other than privacy, is not difficult to implement. However, the responsibilities are broad and require an intricate blend of skills and experience. GPC (Canada) is expected to keep the following in mind when designating such a person:

- the person concerned should have a broad understanding of how personal information is used within the organisation;
-the designated individual may have other responsibilities but not conflicting responsibilities;
- the designated individual should obviously be in a sufficiently high level in GPC (Canada) so that privacy considerations may be articulated at the highest levels of decision-making;
- the designated individual should possess skills for external interactions with government, as well as a broad understanding of the company's internal information management practices.

28. Having developed a code of practice, GPC (Canada) approaches the QMI for registration to Q830. Having already secured a registration to ISO 9001, it judges that the incremental cost and effort of compliance to the privacy standard will be outweighed by the benefits. Organisations applying for registration for Q830 + ISO 9000 Registration are expected to:

- obtain the standard, the application kit and the Workbook[9];
- review all organisational policies and practices;
- submit a documentation package together with the application fee. This documentation shall indicate how they meet the requirements of CAN/CSA-Q830-96 and a national/international standard such as ISO 9001.

QMI will then:

- conduct an audit of the organisation in accordance with ISO 10011 (the international audit standard);
- when the audit has been successfully completed, QMI will then issue the organisation with a letter of Registration and a copy of the 'Statement of Privacy Principles' for signature;
- upon receipt of the duly signed 'Statement of Privacy Principles', QMI will issue the organisation with a QMI Privacy Code Certificate for a three-year cycle;
- once registered, QMI will conduct an annual onsite audit which will cover the ISO 9001 and Q830 elements. The audit team will also record the complaints received and the subsequent actions taken;
- in the third year, QMI will perform a re-registration audit of the organisation, and upon successful completion of the audit will renew the registration for another three-year cycle.

Conclusions

29. The CSA Model Code is potentially a different type of instrument from the typical 'voluntary' code of practice. Standards implementation is based on the very simple adage: 'say what you do, do what you say, and be verified by an independent agency.' The standard has been attractive because of the potential to certify an organisation's policies and practices and thus give a 'good housekeeping seal of approval'. The audit requirements are intended to ensure that high and consistent levels of adherence to data protection principles be maintained, whilst a registration is in force. While registered, the compliance auditing is likely to be more thorough, regular and rigorous than that which can be conducted by under-resourced Privacy Commissioners.

30. Registration to the standard is, however, voluntary. GPC (Canada) takes this step because it believes that it is good business to allay client and government fears in this way. But the registration is of a limited duration, and there is nothing to stop the company from ceasing its registration at any time.

31. Without a registration to the CSA standard, the assessment of adequacy for subcontracted data processing in Canada can only rely on the analysis of the contracts between the client/controller and the processor. Because it has proved impossible to obtain direct access to these contracts in the course of this project, no general conclusions about the scope or content of these contracts can be offered. The limited amount of information available suggests that while there will be some strict security and confidentiality and data integrity provisions in major data processing contracts, they will not meet all of the criteria necessary to provide 'adequate' privacy protection under the EU Data Protection Directive.

---

[9]Canadian Standards Association, *Making the Privacy Code Work for You* PLUS 8830. (Rexdale: CSA, 1996)

32. With the exception of Quebec, the general data protection practices of companies like GPC (Canada) are guided only by non-statutory requirements. If an individual were harmed as a result of personal information processing by a company like GPC, it is difficult to imagine what he/she could do, assuming that the fault could be discovered and blame assigned. The question of remedies for aggrieved data subjects is, therefore, inseparable from that of general compliance with data protection standards set out in instruments such as the CSA Code for the Protection of Personal Information. Bill C-54 is based on the principles contained in the CSA Model Code. To the extent that businesses like GPC transfer personal information interprovincially and internationally, they will be covered by Bill C-54, and remedies will be available through the Federal Privacy Commissioner, and ultimately through the courts.

Sub-contracted Data Processing

(c) *Hong Kong*

The Nature and Circumstances of the Transfer

1. SOUTH CHINA SOLUTIONS (SCS) is a prominent Hong Kong-based company that provides a complete range of information-technology services to a large and diverse range of public and private client organisations. These services include traditional bureau processing, as well as more advanced data warehousing, applications maintenance and network management, all of which will typically involve the handling of customer personal information.

2. All data processing by SCS on behalf of clients is strictly controlled by contract. As a general matter, data processing contracts do not distinguish between personal and non-personal data. If the data are controlled by a client, than the processor has strict obligations for confidentiality. Non-disclosure rules will be designed largely to protect the corporate interest of the client. It is typical practice in the outsourcing industry for such contracts to be shrouded in considerable secrecy, and all guidance about processing is determined by the client through the contract with SCS. It has therefore been impossible to establish what personal data are processed by SCS in Hong Kong, and on what precise terms and conditions.

3. The type of data processed might be any type of personal record routinely processed by computer, such as those relating to telephone bills, credit transactions, health insurance claims, cable television subscriptions, or government taxes or benefits. For the purposes of this case study, GASPLUS is a major utility company (a publicly listed company but partly government owned), operating in several European Union (EU) countries, which contracts with SCS to process its entire customer database in Hong Kong, with daily batch transfers to and from the source countries. The contract between GASPLUS and SCS stipulates that ownership and control of any data processed under the contract (not just any transferred from GASPLUS, but also any collected or generated by SCS) remains with GASPLUS. SCS are constrained to only collect, process, use and disclose data as expressly authorised by GASPLUS or as necessary to perform contractual obligations.

Overview of the Regulatory Environment for This Case

4. SCS in Hong Kong is subject to the Hong Kong Privacy Ordinance 1995, which includes both privacy standards and enforcement and complaint mechanisms, but only in respect of personal information it holds (and in effect controls). Section 2(12) of the Ordinance expressly provides that a person is not a data user (and therefore not subject to the law) in relation to any personal data which the person collects, holds, processes or uses solely on behalf of another person, provided they do not hold, process or use the data for any of their own purposes. In such circumstances (as in this case) the client, and not the contractor is the liable data user. But where the client is an overseas entity, with no local presence, it would be very difficult to enforce the Ordinance.

5. Some Hong Kong government agencies have been including privacy protection clauses in contracts with service providers, particularly in major contracts for IT services and data processing.

Purpose Limitation, Transparency and Opposition

Collection

6. In relation to the collection of customer information, it is assumed that GASPLUS complies with the data protection law of the various European countries in which it operates. The service provided by SCS involves some data about customers being provided directly to SCS by third parties in Europe, such as financial institutions processing direct debit payments, but these again will be subject to the relevant European law. SCS need not take any independent steps to meet fair collection or notification requirements of collection principles, or to obtain the consent required for the collection of any 'sensitive' classes of personal data under Article 8 of the EU Directive.

Use and disclosure by SCS in connection with the contract

7. The processing involved in the performance of the contract is quite complex and includes a variety of matching routines, as well as profiling to generate targeted personalised marketing communications. Customer master records are routinely updated with gas-consumption data provided by GASPLUS and billing information generated and transferred directly to other contractors in Europe for printing and mailing. Again, all of these operations are performed on behalf of GASPLUS under detailed instructions contained in schedules to the contract.

8. The contract specifies that control of any data, including personal information, held by SCS in connection with the contract remains under the control of GASPLUS. Any independent use of the information by SCS would be a breach of contract, and while it would not otherwise be unlawful, it would be subject to the provisions of the Privacy Ordinance.

Disclosure to third parties for their purposes

9. The 'output' data include a variety of returns to government agencies in the source countries; these are transferred by SCS to GASPLUS rather than provided directly.

10. It is difficult to envisage why a Hong Kong government authority would seek access to information about GASPLUS customers held by SCS, but the possibility exists - perhaps as incidental evidence in relation to investigations about SCS's compliance with Hong Kong laws. The requesting agency would have to comply with Hong Kong law including the collection principle of the Privacy Ordinance. For disclosures to third parties in Hong Kong for a purpose of a third party, the SCS is likely to be required by the contract to obtain GASPLUS's express consent, except that the contract would allow SCS to disclose information in an emergency situation where there is a imminent risk to life or health of any person, provided they notify GASPLUS after the event. In all other circumstances, even if there were a legal requirement to disclose within Hong Kong, SCS would refer requests to GASPLUS's legal department. The same would apply to any requests from European authorities, although these would normally be expected to come through GASPLUS in the first place.

Data Quality and Proportionality

11. Regardless of the type of personal data processed under a sub-contract, it is difficult to expect a sub-contractor independently to apply quality standards, other than to ensure data integrity through precautions against inadvertent corruption of the data. Other quality control policies must originate with and be applied directly by the data controller, GASPLUS.

12. SCS is required by the contract to apply a data-retention policy that includes destruction of data after a specified period of time.

Security

13. One area where it is possible to assume that a sub-contract imposes detailed data protection requirements is security. Clients usually have good reasons for protecting their data other than privacy requirements, so it is not surprising that security is a routine feature. Confidentiality requirements are common in data-processing contracts, but details vary widely from contract to contract.

14. While SCS can be expected to offer a fairly high 'base' level of security, additional measures and precautions are likely to be optional, available for a charge, and will depend in this case on what GASPLUS is willing to purchase. Options may include varying levels of backup, disaster recovery, a dedicated security officer, written security requirements, audits, access controls and monitoring, audit trails, and encryption. A large processing company like SCS should be able to provide a great deal of security. Unlike some countries, there are currently no government restrictions in Hong Kong on the level of encryption that can be applied.

Access and Rectification

15. The contract between GASPLUS and SCS would not make any express provision for 'subject' access or correction requests. GASPLUS's customers could be expected to approach the company directly if seeking access. SCS would, on instruction, carry out to meet GASPLUS's requirements for satisfying the relevant European law. If an individual approached SCS directly, then SCS would deal with the request in the same way as any request for disclosure - by referring it to GASPLUS in accordance with the terms of the contract.

Onward Transfer Restrictions

16. Because SCS is not subject to the Privacy Ordinance for data processed on behalf of GASPLUS, Hong Kong law does not prevent SCS from transferring the data to a third country. However, if it did so outside the terms of its contract with GASPLUS, SCS might be open to an action for breach of contract. There would be no point in GASPLUS seeking to include in its contract with SCS a role for the Hong Kong Privacy Commissioner to approve onward transfers, because the Commissioner is not empowered to play such a role in relation to GASPLUS, which is outside his jurisdiction. It would make more sense for the contract to require notification of and approval by the Data Protection Commissioner of the European country from which GASPLUS was transferring data to SCS.

Remedies

17. Express consumer remedies have in the past rarely been included in data processing contracts, although SCS in Hong Kong would have some experience of privacy protection clauses in contracts with HK government and private sector agencies.

18. Unlike in some overseas jurisdictions, Hong Kong law does not recognise any interest by a third party in a contract. If the contract between SCS and GASPLUS were under Hong Kong law, it would not be possible for an aggrieved data subject to use the contract between the data controller and the processor as a basis for a lawsuit against the

processor. This may be an option if the contract was under the law of a European country where the legal system gives third parties these rights.

19. Even if a lawsuit were legally supportable, many barriers remain. First, the contract must contain clauses that were intended to benefit a data subject. If the contract is silent about privacy requirements or unclear about the intended benefits to a data subject, then the lawsuit may fail. For example, contractual security requirements intended to protect a controller's interest in the confidentiality of its data may not create a cause of action by the data subject. The data subject may be an incidental beneficiary with no basis for a lawsuit because the protection of the subject's privacy was not the main purpose of the security requirement. Second, lawsuits are cumbersome and expensive. Foreign nationals might find it to be especially burdensome to sue a Hong Kong company in a Hong Kong court. Third, proving damages in privacy actions is often challenging. Unless a substantial monetary recovery is possible, attracting a lawyer willing to file a lawsuit can be difficult.

20. Even if the SCS/GASPLUS contract could not be enforced directly by an individual, it could in theory contain the same rigorous terms as were required by the German Data Protection Commissioner in the 1995 contract between German National Railways and Citibank in the United States, referred to in the Article 29 Working Party's Working Paper No 9. This provided, for instance, for an individual German complainant to deal throughout the course of a complaint with the German Commissioner and the client organisation, even though the action complained about may have been by the contractor and to have taken place in the United States. But as the Working Party points out, there are many practical difficulties in ensuring that contractual provisions do in fact provide individuals with easily enforceable remedies.

Accountability

21. Given the non-application of the Hong Kong Privacy Ordinance to the data involved in this contract, the contract between SCS and GASPLUS is itself likely to be the only source of any accountability measures in relation to the transferred data. The contract could include provision for such things as SCS's reporting to GASPLUS about its compliance with any data protection terms in the contract, about auditing, about staff training for privacy protection, etc.

Conclusions

22. Under the Hong Kong Privacy Ordinance a 'mere' data processor appears not to be a data controller in relation to personal data processed solely on behalf of another person and is generally therefore not subject to the requirements of the Ordinance (with the possible exception of some of the access and correction provisions). The Ordinance therefore offers no assistance to European data subjects whose information is processed in Hong Kong on behalf of an overseas client.

23. The only source of privacy protection is the contract between client (controller) and processor. Because it has proved impossible to obtain direct access to these contracts in the course of this project, no general conclusions about the scope or content of these contracts can be offered. The limited amount of information available suggests that while there will be some strict security and confidentiality and data integrity provisions in major data processing contracts, they will not meet all of the criteria suggested by the Article 29 Working Party as necessary to provide 'adequate' privacy protection, particularly in terms of remedies and accountability.

Sub-contracted Data Processing

(d) *Japan*

The Nature and Circumstances of the Transfer

1. The GLOBAL PROCESSING CORPORATION (GPC) is a prominent multinational company that provides a complete range of information-technology services to a large and diverse range of public and private client organisations. The services range from the deployment of hardware and software, to user training, to network management, to infrastructure development, to more traditional data management and processing functions. It has thousands of clients in virtually every economic sector in over 40 countries around the world.

2. The analysis for this case does not assume a specific scenario involving the sub-contracted processing in Japan of a particular type of personal data (e.g., consumer data, school records, tax records, telephone billing data, etc.). Instead, the discussion here offers comments on the applicability of laws and codes to several different data types. The type of data processed by a sub-contractor could be any type of personal record routinely processed by computer, including telephone, credit transaction, medical, cable television subscriber, governmental tax, or virtually any other record.

3. All data processing by GPC on behalf of clients is strictly controlled by contract. As a general matter, contracts do not make a distinction between personal and non-personal data. If a client controls the data, then as the processor, GPC has strict obligations for confidentiality and non-disclosure. It is typical practice in the outsourcing industry for such contracts to be shrouded in considerable secrecy, making it impossible to obtain sufficient information about specific processing activities for this study. However, it appears that if an assessment were made solely on the terms of typical contracts, the only fair information practice principle that would be addressed would be security. Contracts do not address notice, subject access, and other principles.

Overview of the Regulatory Environment for This Case

4. No private-sector data protection legislation governs the operations of GPC (Japan). Any data that might be processed under contract with a Japanese government agency is protected under the Act for the Protection of Computer Processed Personal Data held by Administrative Organs of 1988, although this would generally be data on Japanese, rather than overseas, citizens.

5. GPC (Japan) is a full member of the Japan Information Services Industry Association (JISA), a trade association the purpose of which is 'to attain sound and steady growth of the information service industry through the promotion of the development of information-related technology and consolidation of infrastructure for computerization, and to contribute to the economic and social development of Japan through the promotion of computerization'(http://www.jisa.or.jp/introduce/activity-e.html). In 1997, JISA developed ‘Guidelines concerning the protection of computer processed personal data in the information service industry in Japan’, which are consistent with the broader MITI guidelines (http://www.jisa.or.jp/statistics/JISAprivacyguideline-e.html).

6. To secure the actual protection of personal data, Japan Information Processing Development Center (JIPDEC) started the ‘System for Granting Marks of Confidence for Privacy Protection’ from April 1, 1998 (http://www.jipdec.or.jp/security/privacy/pamph-e.html).To get this Privacy Protection Mark (PPM), a company has to submit an application either to JIPDEC or one of the ‘Designated Organisations’, with necessary documentation on the implementation of privacy protection. JISA has been admitted by

JIPDEC as a Designated Organisation for this system, and started accepting applications in August, 1998. If GPC (Japan) seeks the PPM, the relevant standard to which it will be measured is the JISA Guidelines. These guidelines are tailored for information services enterprises such as GPC.

7. For purposes of analysis, it is assumed that GPC (Japan) is currently developing procedures to apply for the PPM. This scenario, at the moment, is hypothetical; no Japanese business has yet to receive the PPM, but several organisations, including those in the data-processing industry, are actively contemplating an application. A variety of incentives might encourage organisations involved in sub-contracted data processing to apply for this 'good housekeeping seal of approval': the desire to avoid adverse publicity or to gain a competitive advantage, pressure from national government, as well as the need to demonstrate an adequate level of protection under European standards.

Purpose Limitation, Transparency and Opposition

Collection

8. The JISA Guidelines contain general language concerning the limitation of collection for the 'legitimate business of information services enterprises'. Collection shall be by lawful and fair means and there are strict stipulations about the collection of data of a sensitive nature. The most relevant section for GPC is the rules concerning the collection of personal data other than from the data subject. Among the exceptions to this rule are '[i]f personal data are collected and disclosed from enterprises with a guarantee that personal data are handled in a manner equivalent to that of the enterprises through conclusion of a contract stipulating the obligation to maintain confidentiality, the prohibition against re-disclosure and the assignment of responsibility when accidents occur in respect of personal data disclosed.'

9. In applying for the PPM, GPC would be expected to specify the purposes of collection and demonstrate that the processing is undertaken according to this standard. GPC would typically have no contact with the data subject and must rely to a certain extent on the legitimacy of the processing undertaken by its clients, who are the data controllers.

Use and Disclosure for GPC Purposes

10. Use-limitation is typically confined in the JISA Guidelines to the following conditions:

- if the data subject has given consent;
- if the use is necessary to permit the data subject to prepare for or to perform a contract to which he is a party;
- if the use is necessary for compliance with legal obligations to which information services enterprises are subject;
- if the use is necessary in order to protect the vital interests of the data subject including life, health, property, etc.
- if the use is necessary for protecting the public interest or for exercising authority under laws by information services enterprises or a third party that personal data are disclosed to;
- if the use is necessary for the legitimate interests of information services enterprises, or a third party or other parties that the personal data are disclosed to, in so far as the interests of the data subject are not infringed.

All other uses must be carried out with the consent of the data subject.

11. In its application, GPC can rely on the justification that sub-contracted data processing constitutes the fulfilment of a legal obligation with its clients. It can also rely on

the somewhat broad argument that it is advancing its 'legitimate interests' as an information service enterprise.

Disclosure to Third Parties for Other Purposes

12. The JISA Guidelines state that 'the disclosure of personal data within the scope of the purpose of the collection shall be carried out with the prior acknowledgement of the data subject secured by obtaining the prior consent of the data subject or by giving the data subject an opportunity to refuse prior to disclosure.' This does not apply, however, 'if personal data are disclosed to the recipient with a guarantee that personal data are handled in a manner equivalent to that of enterprises that disclose the personal data through conclusion of a contract stipulating the obligation to maintain confidentiality, the prohibition against re-disclosure and the assignment of responsibility when accidents occur in respect of personal data disclosed.' This allows GPC (Japan) to sub-contract with other information-processing enterprises under certain circumstances. Disclosures which are outside of the scope of the purpose of collection generally require the consent of data subjects.

13. In the circumstances where GPC (Japan) is approached by a government authority for access to the client's data, prior to the disclosure they are obliged to notify the client of the request, affording the client the right to challenge the access. A typical provision in a contract might read: 'If confidential information is required to be disclosed pursuant to a requirement of a governmental authority, such confidential information may be disclosed pursuant to such requirement so long as the Party required to disclose the confidential information, to the extent possible, provides the other Party with timely prior notice of such requirement and co-ordinates with such other Party in an effort to limit the nature and scope of such required disclosure.'

Data Quality and Proportionality

14. The JISA Guidelines require GPC (Japan) to keep personal data 'accurate and up-to-date to the extent necessary for the purpose of the use.' But no further guidance is given, though organisations would normally be expected to develop guidelines and implement procedures with respect to the retention of personal information.

15. Information that is no longer required to fulfil the identified purposes should be 'destroyed, erased, or made anonymous'. A minimum retention policy should be developed for all categories of personal data collected by GPC (Japan). This will be included in the contract with the client. A typical contractual provision might read: 'Upon written request at the expiration or termination of this Agreement for any reason, all such documented confidential information (and all copies thereof) owned by the requesting Party will be returned to the requesting Party or will be destroyed, with written certification thereof being given to the requesting Party. The provisions of this Section will survive the expiration or termination of this Agreement for any reason.'

Security

16. Echoing the Organisation for Economic Co-operation and Development (OECD) Guidelines, the JISA code simply states that 'reasonable security measures shall be taken through both technical and organisational means against such risks as unauthorised access to personal data or as loss, destruction, alteration, leakage, etc. of personal data.' A range of physical, organisational and technological measures may be appropriate given the sensitivity of the data collected by the company. Further, the JISA Guidelines stipulate that:

> 'In the case where information services enterprises entrust personal data to an outside enterprise, they shall select one that can handle the personal data at a sufficient level of protection, and shall guarantee, through conclusion of a contract or other legal measure,

that the instructions of the manager of the enterprises are observed, that the confidentiality of personal data is maintained, that the re-disclosure of personal data is prohibited, and that responsibility when accidents occur is assigned, and shall maintain the contract, etc. as written documents or magnetically-stored records for the period that the personal data are managed by the outside enterprise.'

17. Organisations are also expected to remind employees constantly of the importance of maintaining the confidentiality of such information. All such safeguards and measures should be openly stated.

18. As a general matter, client contracts include security requirements. The applicable contractual commitments are supposed to be communicated to the employees responsible for their implementation. Contracts also stipulate clear procedures for audits in terms of their scope and procedures. Access controls are routinely used to identify wrongful access or attempts to access data. With its mainframe applications, GPC (Japan) also implements audit trails to record both internal and external access. Whether or not encryption is used depends on the specific requirements and the contractual provisions. All physical, technological and organisational security measures have to be described in GPC's application to the PPM.

Access and Rectification

19. Given the only indirect relationship between the data subject and GPC (Japan), the access and correction rights contained in the JISA Guidelines would only be of academic interest. The Guidelines also permit a data subject to refuse the use or disclosure of personal data managed by information services enterprises. If GPC (Japan) received such a request it would presumably argue that it is performing obligations under laws and contract and that if anybody has an obligation to provide access, it is the client/controller, depending on whether that organisation is governed by other data protection legislation.

Onward Transfer Restrictions

20. No restriction on onward transfers appears to be included in the JISA guidelines or in any legislation. Provided the organisation uses contractual or other means to provide a comparable level of protection while the information is being processed by a third party, the transfer is permissible. Thus, if GPC (Japan) used a sub-contractor to process some of the personal data for some clients, it would be responsible for ensuring that the sub-contractor would also conform to the privacy standard.

21. The client contract may also stipulate procedures or limitations respecting the location of processing. In some cases local laws may be a consideration, restricting or prohibiting certain transfers. These laws are frequently not premised upon privacy principles, but rather principles of national security (e.g., military classified information) or political considerations (e.g., taxpayer information). The realities of the data processing transaction dictates that the client-controller of the data maintain control of the data and any uses to which they are put. Frequently GPC (Japan) is allowed a degree of latitude in determining specifics of the processing, but it never exercises control over the uses of the client's data.

Remedies

22. Any consumer may register a complaint with the granting organisation (in this case JISA), about the practices of a company that has been awarded the PPM. The granting organisation is then expected to take the appropriate action in consultation with the

enterprise concerned. This process is inextricably linked, however, to the system for awarding PPMs, and does not seem to be available in relation to any enterprise that has not already received the Mark (http://www.jipdec.or.jp/security/privacy/pamph-e.html).

Accountability

23. The privacy-mark system is operated by the PPM-granting organisation (JIPDEC) and other Designated Organisations, including JISA. The granting organisation is responsible for examining private enterprises' applications for the PPM, certifying them, and operating this system appropriately. A Privacy Mark System Committee, consisting of experts, representatives of business groups, representatives of consumers, lawyers, and so on and is responsible for ensuring the integrity of the entire regime.

24. The PPM is granted to a private enterprise that has one or more business establishments in Japan. Besides the above requirement, an enterprise must develop a code of practice complying with MITI's 'Guidelines for Protection of Personal Information Related to Computer Processing in the Private Sector' (MITI Notification No. 98 on March 4, 1997), or the industry guidelines, based on the Guidelines, established by the business group to which the enterprise belongs (such as those from JISA). It must then demonstrate that personal information is appropriately managed, based on the code of practice, or that a feasible structure has been established. The JISA Guidelines also require the appointment of a manager for personal information, and stipulate the duties of such a person.

25. In applying for the PPM, the enterprise must: (a) accurately specify the parts of the organisation to which privacy protection will apply; and (b) submit completed application forms together with the fee to the Designated Organisation. The accepted application documents are examined based on the separately provided 'Privacy Mark Granting Certification Standard'. These are compared against the code of practice and other operational guidelines established for protecting personal information, and the internal administrative structure established for compliance with these guidelines.

26. The Designated Organisation will, in particular, check that:

- a structure for appropriately handling personal information is established. For example, a manager of personal information is appointed and the internal responsibility and the division of roles related to protection of personal information are made clear;
- training measures are taken at least once a year for those who collect, use, or provide personal information;
- the personal information practices of the enterprise are audited at least once a year;
- the enterprise has a permanent contact point for consultation related to its protection of personal information, and this contact point is clearly indicated to consumers;
- appropriate security measures are taken for personal information owned by the enterprise to prevent theft by outsiders and leaks by insiders; and
- when an enterprise provides personal information to an external organisation or subcontracts its handling, it takes measures for appropriately protecting personal information by concluding a contract related to the division of responsibilities and confidentiality.

27. If any doubt arises during an examination, an applicant is sometimes asked to provide other necessary information by means of a hearing. In some cases, the business operations may be examined by an on-site investigation. When a decision to approve or reject the certification is made based on the examination, a notice of privacy mark-granting examination showing the result is sent to the applicant. When an applicant receives a notice of approval and deposits the charge for using the PPM for two years to the granting organisation by the specified date, the granting organisation grants a privacy mark certificate to the enterprise. This is promptly announced on the home page of the granting organisation. A certification is effective for two years. The PPM is strictly protected by

trademark law and can only be displayed by organisations that have followed the foregoing procedure.

28. In some cases, the granting organisation and a designated organisation ask a PPM-certified enterprise to report an audit result related to the handling of personal information. It is also envisaged that JIPDEC would ask a designated organisation to report the actual state of privacy mark certification as necessary. In some cases, the granting organisation and the designated organisation that receives such a report might demand an on-site study of an enterprise. This might lead to the cancellation of certification of an enterprise, or of the designation of a designated organisation.

Conclusions

29. The Privacy Protection Mark (PPM) is potentially a very effective method by which organisations can demonstrate compliance with privacy protection principles. The regime combines a standardised system for developing codes of practice with a clear process of conformity assessment. Like the Canadian Standards Association (CSA) privacy standard in Canada, it represents a step above the traditional privacy code of practice. It may be a most useful method by which the adequacy of privacy protection can be assured in Japan, when data on European citizens is transferred to Japan for processing.

30. Enterprises such as GPC (Japan) might have a considerable interest in adopting the PPM. Its trade association (JISA) is a designated organisation with delegated authority to receive applications. The sensitivity of the data processed by companies like GPC (Japan) suggests that the desire to demonstrate compliance with fair information practices might be quite strong.

31. However, the system is new and untested. Moreover, it can be predicted that, at the outset at least, only the more responsible organisations will make the effort to seek the PPM. Only time will tell whether a critical mass of organisations within a particular sector will be awarded this ‘good housekeeping seal of approval’, thus isolating free-riders. Remedies for consumers are also closely tied to this process. It is difficult to understand how individuals might use this system to seek redress against an organisation that has not applied for the Mark, and has no intention of doing so.

Sub-contracted Data Processing

(e) *New Zealand*

The Nature and Circumstances of the Transfer

1. SOUTHERN CROSS DATA PROCESSORS (SCDP) is a prominent New Zealand- based company that provides a complete range of information technology services to a large and diverse range of public and private client organisations. These services include traditional bureau processing, as well as more advanced data warehousing, applications maintenance and network management, all of which will typically involve the handling of customer personal information.

2. All data processing by SCDP on behalf of clients is strictly controlled by contract. As a general matter, data processing contracts do not distinguish between personal and non-personal data. If the data are controlled by a client, than the processor has strict obligations for confidentiality. Non-disclosure rules will be designed largely to protect the corporate interest of the client. It is typical practice in the outsourcing industry for such contracts to be shrouded in considerable secrecy, and all guidance about processing is determined by the client through the contract with SCDP. It has therefore been impossible to establish what personal data are processed by SCDP in New Zealand, and on what precise terms and conditions.

3. The type of data processed might be any type of personal record routinely processed by computer, such as those relating to telephone bills, credit transactions, health insurance claims, cable television subscriptions, or government taxes or benefits. For the purposes of this case study, UTILCORP is a major utility company (a publicly listed company but partly government owned), operating in several European Union (EU) countries, which contracts with SCDP to process its entire customer database in New Zealand, with daily batch transfers to and from the source countries. The contract between UTILCORP and SCDP stipulates that ownership and control of any data processed under the contract (not just any transferred from UTILCORP, but also any collected or generated by SCDP) remains with UTILCORP. SCDP is constrained to only collect, process, use and disclose data as expressly authorised by UTILCORP or as necessary to perform contractual obligations.

Overview of the Regulatory Environment for This Case

4. SCDP in New Zealand is subject to the New Zealand Privacy Act 1993, which includes both privacy standards and enforcement and complaint mechanisms, but only in respect of personal information it holds (and in effect controls). Section 3(4) of the Act expressly provides that where an agency holds information "for the sole purpose of processing the information on behalf of another agency, and does not use or disclose the information for its own purposes", then the information is deemed to be held by the 'client' agency. Where the client is an overseas entity, the Act arguably still applies but enforcement may be difficult (see below). Although the effect of s.3(4) has not yet been tested in the courts, it appears that an IT contractor like SCDP would not be subject to the New Zealand Act in relation to data not processed on behalf of UTILCORP.

5. Some New Zealand government agencies have been including privacy protection clauses in contracts with service providers, particularly in major contracts for IT services and data processing. The Privacy Commissioner issued a Code of Practice for the company then providing IT services to the government in 1994, and in 1997 issued a replacement Information Privacy Code following the takeover of that company by another.

Purpose Limitation, Transparency and Opposition

Collection

6. In relation to the collection of customer information, it is assumed that UTILCORP complies with the data protection law of the various EU countries in which it operates. The service provided by SCDP involves some data about customers being provided directly to SCDP by third parties in Europe, such as financial institutions processing direct debit payments, but these again will be subject to the relevant European law. SCDP need not take any independent steps to meet fair collection or notification requirements of collection principles, or to obtain the consent required for the collection of any 'sensitive' classes of personal data under Article 8 of the EU Directive..

Use and disclosure by SCDP in connection with the contract

7. The processing involved in the performance of the contract is quite complex and includes a variety of matching routines, as well as profiling to generate targeted personalised marketing communications. Customer master records are routinely updated with energy-consumption data provided by UTILCORP and billing information generated and transferred directly to other contractors in Europe for printing and mailing. Again, all of these operations are performed on behalf of UTILCORP under detailed instructions contained in schedules to the contract.

8. The contract specifies that control of any data, including personal information, held by SCDP in connection with the contract remains under the control of UTILCORP. Any independent use of the information by SCDP would be a breach of contract, and while it would not be unlawful under any New Zealand statute, it would be subject to the provisions of the Privacy Act.

Disclosure to third parties for their purposes

9. The 'output' data include a variety of returns to government agencies in the source countries; these are transferred by SCDP to UTILCORP rather than provided directly.

10. It is difficult to envisage why a government authority in New Zealand would seek access to information about UTILCORP customers held by SCDP, but the possibility exists - perhaps as incidental evidence in relation to investigations about SCDP's compliance with New Zealand laws. For disclosures to third parties in New Zealand for a purpose of a third party, the SCDP is likely to be required by the contract to obtain UTILCORP's express consent, except that the contract would allow SCDP to disclose information in an emergency situation where there is a imminent risk to life or health of any person, provided they notify UTILCORP after the event. In all other circumstances, even if there were a legal requirement to disclose within New Zealand, SCDP would refer requests to UTILCORP's legal department. The same would apply to any requests from European authorities, although these would normally be expected to come through UTILCORP in the first place.

Data Quality and Proportionality

11. Regardless of the type of personal data processed under a sub-contract, it is difficult to expect a sub-contractor independently to apply quality standards, other than to ensure data integrity through precautions against inadvertent corruption of the data. Other quality control policies must originate with and be applied directly by the data controller, UTILCORP.

12. SCDP is required by the contract to apply a data-retention policy that includes destruction of data after a specified period of time.

Security

13. One area where it is possible to assume that a sub-contract imposes detailed data protection requirements is security. Clients usually have good reasons for protecting their data that go beyond privacy requirements, so it is not surprising that security is a routine feature. Confidentiality requirements are common in data-processing contracts, but details vary widely from contract to contract.

14. While SCDP can be expected to offer a fairly high 'base' level of security, additional measures and precautions are likely to be optional, available for a charge, and will depend in this case on what UTILCORP is willing to pay for. Options may include varying levels of backup, disaster recovery, a dedicated security officer, written security requirements, audits, access controls and monitoring, audit trails, and encryption. a large processing company like SCDP should able to provide a great deal of security. Unlike some countries, there are currently no government restrictions in New Zealand on the level of encryption that can be applied.

Access and Rectification

15. The contract between UTILCORP and SCDP would not make any express provision for 'subject' access or correction requests. UTILCORP's customers could be expected to approach the company directly if seeking access. SCDP would, on instruction, carry out to meet UTILCORP's requirements for satisfying the relevant European law. If an individual approached SCDP directly, then SCDP would deal with the request in the same way as any request for disclosure - by referring it to UTILCORP in accordance with the terms of the contract.

Onward Transfer Restrictions

16. New Zealand law does not prevent SCDP from transferring the data its processes on behalf of UTILCORP to a third country, but if it did so outside the terms of its contract with UTILCORP it would lay itself open to a breach of contract action. The Code issued by the Privacy Commissioner in 1997 for the outsourced government computing services specifically prohibits the transfer of specified personal information out of New Zealand without written authorisation from the relevant government department, and without notification of the destination and appropriate safeguards to the Privacy Commissioner. There would be no point in SCDP including similar provisions in its contract with UTILCORP, because the New Zealand Privacy Commissioner is not empowered to play the same role in relation to UTILCORP, which is outside his jurisdiction. It would make more sense for the contract to require notification of and approval by the Data Protection Commissioner of the European country from which UTILCORP was transferring data to SCDP.

Remedies

17. Express consumer remedies have in the past rarely been included in data processing contracts, although SCDP in New Zealand would have some experience of privacy protection clauses in contracts with New Zealand government and private sector agencies. These have included a requirement for the contractor to co-operate with any investigation into an alleged breach of privacy, and to notify the client of any consumer complaint.

18. Unlike most common law jurisdictions, New Zealand law does recognise interests of third parties in contracts (Contracts (Privity) Act 1982). If the contract between SCDP and UTILCORP were under New Zealand law, and made appropriate provision, it would be possible for an aggrieved data subject to use the contract between the data controller and the processor as a basis for a lawsuit against the processor. This may also be an option if the contract were under the law of a European country where the legal system similarly gives third parties these rights.

19. Even if a lawsuit were legally supportable, many barriers remain. First, the contract must contain clauses that were intended to benefit a data subject. If the contract is silent about privacy requirements or unclear about the intended benefits to a data subject, then the lawsuit may fail. For example, contractual security requirements intended to protect a controller's interest in the confidentiality of its data may not create a cause of action by the data subject. The data subject may be an incidental beneficiary with no basis for a lawsuit because the protection of the subject's privacy was not the main purpose of the security requirement. Second, lawsuits are cumbersome and expensive. Foreign nationals might find it to be especially burdensome to sue a New Zealand company in a New Zealand court. Third, proving damages in privacy actions is often challenging. Unless a substantial monetary recovery is possible, attracting a lawyer willing to file a lawsuit can be difficult.

20. Even if the SCDP/UTILCORP contract could not be enforced directly by an individual, it could in theory contain the same rigorous terms as were required by the German Data Protection Commissioner in the 1995 contract between German National Railways and Citibank in the United States, referred to in the Article 29 Working Party's Working Paper No 9. This provided, for instance, for an individual German complainant to deal throughout the course of a complaint with the German Commissioner and the client organisation, even though the action complained about may have been by the contractor and to have taken place in the United States. But as the Working Party points out, there are many practical difficulties in ensuring that contractual provisions do in fact provide individuals with easily enforceable remedies.

Accountability

21. UTILCORP is subject to accountability requirements in its home country. Given the non-application of the New Zealand Privacy Act to the data involved in this contract, the contract between SCDP and UTILCORP is itself likely to be the only source of any accountability measures in relation to the transferred data. The contract could include provision for such things as SCDP's reporting to UTILCORP about its compliance with any data protection terms in the contracts, about auditing, about staff training for privacy protection, etc.

Conclusions

22. The New Zealand Privacy Act does not apply to 'mere' data processors and offers no assistance to European data subjects whose information is processed in New Zealand on behalf of an overseas client, except in respect of any unauthorised uses, which would also be a breach of contract.

23. The only source of privacy protection is the contract between client (controller) and processor. Because it has proved impossible to obtain direct access to these contracts in the course of this project, no general conclusions about the scope or content of these contracts can be offered. The limited amount of information available suggests that while there will be some strict security and confidentiality and data integrity provisions in major data processing contracts, they will not meet all of the criteria suggested by the Article 29 Working Party as necessary to provide 'adequate' privacy protection, particularly in terms of remedies and accountability.

Sub-contracted Data Processing

(f) *United States of America*

The Nature and Circumstances of the Transfer

1. The OUTSOURCING CORPORATION OF AMERICA (OCA) is a large multinational company that provides a complete range of information technology services to a diverse class of public and private client organisations. The services include the deployment of hardware and software, user training, network management, infrastructure development, traditional data management, and computer processing functions. It has thousands of different clients in virtually every economic sector in over 40 countries around the world.

2. For this reason, the present discussion does not assume a specific scenario involving the sub-contracted processing in the United States of a particular type of personal data originating from data controllers in countries of the European Union (EU). The type of data processed by a sub-contractor could be any type of personal record routinely processed by computer, including telephone billing, credit transaction, medical records, cable television subscriber information, other kinds of personal consumer data, school records, governmental tax, or virtually any other record. The discussion below comments on the applicability of laws and codes to several different data types.

3. All data processing by OCA on behalf of clients is strictly controlled by contract. As a general matter, data processing contracts do not distinguish between personal and non-personal data. If the client controls the data being processed, then the processor is likely to have strict obligations for confidentiality. The main purpose of contract provisions requiring non-disclosure is to protect the corporate interests of the client. Contracts in the outsourcing industry are typically shrouded in considerable secrecy, making it impossible to obtain sufficient information about specific processing activities for this study.The client determines all processing details through its contract with OCA. However, it appears that if an assessment were made solely on the terms of typical contracts, the only fair information practice principle that would be addressed would be security. Contracts do not address notice, subject access, and other principles.

Overview of the Regulatory Environment for This Case

4. Elsewhere in this Report, the Canadian scenario for sub-contracting records assumes that the sub-contractor has registered to the ISO 9001 quality assurance standard and is working to bridge the Canadian Standards Association Model Code for the Protection of Personal Information to that standard. For the United States, it is difficult to propose a similar hypothetical case.

5. The United States has no general privacy standards in law, and no single self-regulatory code in place or in development can readily be used as a model. Self-regulatory efforts in the United States are underway for various industries. However, for most of these efforts, self-regulatory standards are either still in the process of formation or are too new to evaluate. It may be some time before it is possible to assess how companies are actually applying the self-regulatory standards in practice.

6. Starting in 1997, the United States Department of Commerce began to encourage industry to adopt and implement *effective* self-regulatory fair information practice codes. This attention to fair information practices is part of a larger project on global electronic commerce. Other federal agencies are also examining similar issues. A June, 1998 study by the United States Federal Trade Commission (FTC) about commercial Internet website compliance with privacy standards found that most collected personal information.

However, only fourteen percent provided any consumer notice of information practices, and only two percent offered consumers a comprehensive privacy policy. Compliance with privacy standards in the non-Internet world may be even worse.

7. In the United States, no specific self-regulatory code is in place for the class of data processors that offer computer services. Some companies engaged in multinational subcontracting have enrolled as sponsors of some new privacy self-regulatory efforts, and many belong to trade associations that may also prescribe self-regulatory codes. None of the self-regulatory efforts, however, expressly addresses client data being processed by subcontractors. A data processor can commit itself to follow specific privacy practices of its own choice. Yet it is difficult to see how a processor can attract business if it insists that its own privacy rules, rather than the rules prescribed by the customer, must apply to customer data.

8. In theory, at least, the patchwork quilt of United States privacy laws and self-regulatory efforts might occasionally apply to foreign data processed in the United States. For the most part, however, whatever American protections exist apply to American record keepers processing data on United States citizens. It is difficult to find many American privacy laws that bring within the scope of their coverage data on foreigners that were imported solely for processing purposes. In the main, questions about the applicability of laws to imported data have rarely, if even, been considered.

9. Because of the limits of United States laws and the inability obtain access to actual data processing contracts, the discussion here will focus on how United States laws and self-regulatory codes might apply (if at all) to personal data brought to the United States for processing. The goal is to assess whether the American systems of sectoral laws and developing self-regulatory codes offer any formal protections for personal data imported from European Union (EU) countries.

Purpose Limitation, Transparency and Opposition

10. If OCA received a contract to undertake processing of consumer reporting records of, for example, an EU-based credit-reporting company, would the American Fair Credit Reporting Act impose any restrictions on processing functions or otherwise provide any protections for data subjects? The Fair Credit Reporting Act (FCRA) was the first major federal data protection law in the United States. The Act became law in 1970 and was amended significantly in 1996. It addresses all elements of fair information practices. For example, the FCRA specifies the permissible purposes for which consumer reports may be used and disclosed. The law also requires that consumer-reporting agencies must notify consumers about the activities of the agencies and about the right of consumers. Whether these provisions of the FCRA would fully meet EU standards is uncertain, but there is no need to make a determination here because it is not clear that the provisions are applicable at all.

11. The FCRA's requirements apply to *consumer-reporting agencies*. That term includes any person regularly engaged in the practice of assembling or evaluating consumer-credit information for the purpose of furnishing consumer reports to third parties. The law does not explicitly limit applicability to American companies or to American consumer-reporting agencies. A company located in another country that performed consumer-reporting functions about United States consumers would be subject to the law if that company were engaged in interstate commerce within the United States. A company within the United States that provided consumer-reporting services on foreign nationals residing or engaging in commerce within the United States would also be subject to the law. A specific consumer record transferred to an American credit reporting agency by an EU-based credit reporting company would also fall under the protections of the United States law once in the possession of the American firm.

12. The mere processing of foreign consumer reports within the United States does not, however, appear to bring the processor within the scope of the law. OCA would not be considered to qualify as a consumer-reporting agency under the terms of the FCRA because it does not furnish consumer reports to third parties. The company that hired the processor might arguably be subject to the FCRA if that company performed enough of its credit-reporting activities within the United States, but that conclusion is by no means certain. Simply hiring OCA to process consumer credit data would probably not establish enough of a nexus to bring the data or the processor under the FCRA.

13. These conclusions about the applicability of the FCRA to international activities are, however, speculative. Questions about the international scope of the law have not arisen or been considered in the United States. The drafters of the credit-reporting law did not consider international applicability issues, and nothing in the text of the law addresses application to sub-contractors of foreign consumer-reporting agencies. It is typical that American privacy laws are silent on international applicability issues. It is nevertheless reasonable to conclude that the limitations on data use and protections for data subjects in the American law would be inapplicable in most cases to an American sub-contractor for an EU-based consumer-reporting agency. Consequently, the contract between an American firm and an EU-based consumer-reporting company remains the only likely source of any fair information practice requirements.

Data Quality and Proportionality

14. Regardless of the type of personal data processed under a subcontract, it is difficult to expect a sub-contractor independently to apply quality standards and collection limitations. These policies must originate with and be applied directly by the data controller. For example, a subcontractor might be directed in the contract to apply data-retention rules requiring that data be discarded after a specified period when there is no longer any need for the data. The source of the retention rules, however, could only be the contract and the data controller.

15. A new set of self-regulatory guidelines released in June 1998 illustrates this point. The Online Privacy Alliance (http://www.privacyalliance.org) is a voluntary organisation of over 50 companies that agreed to support self-regulation for privacy and to comply with common privacy guidelines. The companies participating in the Online Privacy Alliance include International Business Machines, Electronic Data Systems, Microsoft, Ernst & Young, and Price Waterhouse.

16. The policies for the Online Privacy Alliance apply to the protection of individually identifiable information in an online or electronic commerce environment. One policy addresses data quality and access. It begins: 'Organizations creating, maintaining, using or disseminating individually identifiable information should take reasonable steps to assure that the data are accurate, complete and timely for the purposes for which they are to be used.'

17. How this policy would apply to data under a sub-contract is not clear. First, it is not certain that a subcontractor processing data qualifies as an organisation 'creating, maintaining, using, or disseminating individually identifiable information.' Second, even if it does qualify, the application of the purpose test is undefined. Would a subcontractor be bound to apply the purpose test from the perspective of the data controller or from its own perspective? The former would appear possible only if the data controller established quality standards in the contract. The latter reading would have little effect since the purpose of the processing is processing. Any constraints suggested by the policy would not be meaningful from the perspective of the data subject.

18. The introduction to the Online Privacy Alliance guidelines states that the policies may be customised as appropriate to any business or industry sector. How this general

qualification might be applied in any specific context is not clear. Even if both a controller and its processor subscribed to the same guidelines, a policy that applies to a controller may not be 'appropriate' for a data processor. Pending further clarification or developments, the self-regulatory guidelines present the same threshold uncertainties that American privacy laws do. It is not clear that they offer any meaningful consumer protections when sub-contractors process personal data.

Security

19. One area where it appears safe to assume that a sub-contract will impose at least some requirements is security. Confidentiality requirements are reported to be common in processing contracts, but details vary widely from contract to contract. The degree of security may depend on what level of protection the controller is willing to purchase. Options may include extensive safeguarding, backup, disaster recovery, a dedicated security officer, written security requirements, audits, access controls and monitoring, audit trails, and encryption. Data processors are likely to be willing to provide as much security as the customer can afford. Laws and polices that address security for personal data tend to have very general requirements (e.g., 'reasonable safeguards'), so that it is difficult to assess specific needs in the absence of a context. Nevertheless, companies like OCA have good reasons for protecting their data that go beyond privacy requirements, so it is not surprising that security is a routine feature.

Access and Rectification

20. If the sub-contract involved the processing of school records from an EU school by OCA, the federal law that expressly provides rights of access and correction for school records would clearly not apply. The Family Educational Rights and Privacy Act (also known as the *Buckley Amendment*) applies to elementary and secondary schools and to colleges and universities receiving federal funds. The United States Secretary of Education enforces the law by withdrawing federal financial support from schools that do not meet the law's requirements. American schools that do not receive federal funds are not subject to the law. A non-United States school would not be subject to the law for the same reason. Because the requirements of the law apply to schools and not directly to student records, the law offers no protections to student records imported into the United States for processing. Thus, only the contract between the data controller and OCA could provide any access or correction rights to data subjects.

21. The same conclusion applies to one of the few other federal laws that establishes a right of access to personal records by data subjects. The Cable Communications Policy Act of 1984 requires companies offering cable services in the United States to grant access and correction rights to subscribers. If records of a European cable television service company that provided services in Europe were processed in the United States, the records would not be subject to the cable law. The act of processing information about cable television subscribers would not appear to be sufficient for OCA to qualify as a cable operator.

Onward Transfer Restrictions

22. For at least one class of EU-based records processed in the United States, a privacy law might apply. The Video Privacy Protection Act expressly references foreign commerce. The law applies privacy requirements to *video tape service providers*, and this term includes those who affect foreign as well as interstate commerce. The requirement also would apply to any person who obtains records from a video tape service provider 'in the ordinary course of business.' Thus, an American processor who performs debt-collection activities, order-fulfilment, request processing, or the transfer of ownership on behalf of an

EU-based company would likely be subject to the relatively strict transfer restrictions in the Video Privacy Protection Act. These restrictions require consent or a court order before any transfer.

23. The Video Privacy Protection Act would not necessarily prevent the transfer of information to another jurisdiction, although the law's disclosure restrictions might continue to apply to the information in that jurisdiction. Express restrictions on the transfer of sub-contracted data to other jurisdictions would have to be found in the contract. It is possible or even likely that in the absence of a specific restriction, personal data maintained by a sub-contractor could be transferred to another jurisdiction or accessible in another jurisdiction over a computer network. In the case of video records, at least, United States law might continue to apply. Conclusions about foreign applicability of the video privacy law are speculative because the issues have never been raised or litigated.

Remedies

24. Occasional statutory remedies for privacy violations, such as the remedy provided by the Video Privacy Protection Act, may exist in the United States. However, many important categories of personal records are unprotected by federal privacy laws. Health, insurance, employment, and marketing records are subject to scattered and limited laws that rarely address the full range of fair information practices even when the laws exist. Even where statutory remedies exist, it is unlikely that they would be available to a foreign data subject whose information is processed by OCA on behalf of a European company. Common law or statutory tort actions for privacy violations can be maintained in many states, but the remedies available do not address most fair information practice goals. In some instances, aggrieved data subjects may be able to recover money damages. For the most part, however, successful privacy tort actions are rare. A lawsuit on behalf of a foreign data subject against an American data processor would be novel.

25. One question that would surely arise in any litigation by a data subject brought under a contract to which the data subject is not a party is whether that data subject has sufficient legal interest – or privity – to be able to sustain the lawsuit. A lack of privity can sometimes be a barrier to a lawsuit. However, under current contract-law principles, a contract with privacy clauses that benefit a data subject who is not a party to the contract may still be enforceable by the data subject. The general conditions are that the parties to the contract intended the data subject to benefit and that enforcement by the data subject is appropriate to achieve the intent of the parties. In other words, a data subject may be able to sue to enforce data protection provisions of a contract although the data subject is not a party to the contract. A finding of sufficient legal interest does not guarantee success in a lawsuit, but the absence of sufficient legal interest can be fatal. Contract law varies from state to state so that the general American rule on privity may not apply in every state. Even if a lawsuit is possible, the scope of available relief may be severely limited. If the only fair information practice principle incorporated in the contract is data security, then the only ground for the lawsuit may be a breach of the security obligation. Other fair information practice standards may not be achievable by a data subject under a lawsuit.

26. Even if a lawsuit is legally supportable, many barriers remain. First, the contract must contain clauses that were intended to benefit a data subject. If the contract is silent about privacy requirements or unclear about the intended benefits to a data subject, then the lawsuit may fail. For example, contractual security requirements intended to protect the controller's interest in the confidentiality of its data may not create a cause of action by the data subject. The data subject may be an incidental beneficiary with no basis for a lawsuit because the protection of the subject's privacy was not the main purpose of the security requirement. Second, lawsuits are cumbersome and expensive. Foreign nationals might find it especially burdensome to sue an American company in a United States court. Third,

proving damages in privacy actions is often challenging. Unless a substantial monetary recovery is possible, attracting a lawyer willing to file a lawsuit can be difficult.

Accountability

27. The United States does not have omnibus privacy legislation or an American equivalent to a data protection agency. Existing agencies with sectoral responsibilities can enforce or oversee specific privacy laws, although it is more common for the laws to be enforced through private litigation. The FTC may have the broadest potential reach. It may be able to enforce privacy self-regulatory codes for some industries. However, examples of administrative enforcement efforts for privacy are rare. In August 1998, the FTC brought its first Internet privacy enforcement action. The full scope of the FTC's jurisdiction over fair information practices is controversial. In any event, the Commission may not recognize the full range of fair information practices. A June 1998 FTC report on Internet privacy only recognized notice/awareness, choice/consent, access/participation, integrity/security, and enforcement/redress as elements of fair information practices.

28. Industry codes might require dispute resolution, self-assessment, or independent audits. American privacy self-regulatory efforts are still developing. As mentioned above, the Online Privacy Alliance adopted general policies in June 1998. A subsequent policy statement concluded that the effective enforcement of self-regulation requires: 1) verification and monitoring, 2) complaint resolution and 3) education and outreach. These mechanisms for enforcement and accountability have not yet been established or implemented. It remains to be seen how many American companies will subscribe to the Online Privacy Alliance standards or how many subscribers will actually follow the standards. The nature of the enforcement and accountability measures is also uncertain.

29. At present, the main or most likely source of any effective fair information practice accountability measures will be the contract between an American processor and the EU-based data controller. Express consumer remedies are likely to be rarely, if ever, included in data processing contracts. However, an aggrieved data subject may be able use the contract between the data controller and the processor as a basis for a lawsuit against the processor, although the only likely relief may be for breach of security obligation.

Conclusions

30. It is impossible to offer any general conclusions about adequacy of data protection when an American company, such as OCA, processes data on behalf of an EU-based data controller. For the most part, American statutes and common law impose few requirements on data processors and offer little or no assistance to data subjects. Even where laws exist, they are likely not to be applicable to data that are processed in the United States. The scope and degree of processing may make a difference to the applicability of American privacy laws in some instances, however. If the American data processing company performs enough substantive processing, it is possible that the activity could fall under American laws or self-regulatory guidelines in some cases. In the end, however, American privacy laws remain a patchwork quilt, with protection available only for narrow classes of data.

31. The only other source for assessment of privacy protections is the contract between controller and processor. Because it has proved impossible to obtain direct access to these contracts in the course of this investigation, no general conclusions about the scope or content of these contracts can be offered. It is likely that security receives significant attention. The limited amount of information available suggests that other aspects of privacy are rarely addressed in data processing contracts.

32. Subcontracting activities do not measure well against the three enforceability criteria suggested by the EU. For the most part, no relevant law or code can be identified. No system of support for data subjects can be found. A very limited remedy for some violations of one fair information practice principle may be possible. The most likely source for compliance with these criteria will have to be the contract itself and oversight by the data controller who awarded the contract, and it appears that most contracts are silent on data protection.

Conclusions about Sub-Contracted Data Processing

1. Transfers of personal data between data controllers and data processors pursuant to sub-contracts are, for the most part, wholly unregulated. Even in those jurisdictions that have general private-sector data protection laws, the laws are generally not applicable to data processors who do not make independent use of data. In some jurisdictions, laws that might apply to data processed about citizens or residents of the jurisdiction are not likely to apply to similar data imported solely for processing.

2. The wide scope of sub-contracted processing makes it impossible to offer any general conclusions about the extent to which industry practices meet European Union standards. Outside assessors cannot obtain specific information about contracts that are, for the most part, shrouded in secrecy both as to their terms and the nature of the processing undertaken. This category of transfers therefore presents a significant challenge for the assessment of adequacy. Except for security, where there is reason to believe that high standards are commonplace, it is extremely difficult to determine how far compliance with other fair information practices is addressed.

3. However, because the processed data necessarily originate with a European organisation that is subject to a 'home country' data protection law, a full set of protections for data subjects should be available under the law of that country. Whether there is a need for a full set of data protections for individuals whose data are only being processed abroad is unclear, although some protections against misuse outside the terms of any contract are surely needed. Appropriate solutions for protecting data transferred abroad for processing may be narrower than for other categories. It is beyond the scope of this study to estimate the extent to which contractual solutions offer a way forward.

III. METHODOLOGICAL CONCLUSIONS

Introduction

1. In this Section, we discuss our experiences in conducting the investigations for this Report and reach conclusions about the application of the methodology for assessing the adequacy of privacy protection in third countries. We also comment upon a range of issues that will be important for any future assessments of this kind, and that should be considered in the implementation of the European Union Data Protection Directive.

2. The Introduction to this Report describes the origins and scope of this investigation. The inventory of questions used in the case studies appears in an Appendix.

3. The preparation of this Report was considerably more challenging than was initially anticipated. The difficulties encountered may be instructive to others who engage in similar assessments of adequacy.

4. Despite the practical difficulties, discussed below, we are confident that this Report addresses realistic transfer scenarios as they are occurring in 1998. For the most part, the case studies analyse similar transfers of data to the six jurisdictions, thereby allowing at least a broad comparative assessment of the adequacy of protection in those countries, sector by sector. Deeper investigation would, no doubt, cast more light on the extent of actual compliance with data protection principles in these different sectors and in the various countries, but we believe that this Report provides a very useful basis for such further enquiry. Effective decision-making concerning the permissibility of transfers of personal data to third countries can be achieved in a number of ways. However, to the extent that it is to be based upon the reasoning adopted by the Directive and by institutions of the European Union, a more thorough analysis is desirable.

5. The literature on the implementation of the Directive has been heavily dominated by analyses of legal norms and rules. We would argue that a more empirical analysis of policies and practices, as well as rules, serves both to advance the debate and to anticipate the specific problems that will be encountered in the implementation of the Directive. That is what we try to accomplish in this Report. We also maintain that the assessment of adequacy will be incomplete to the extent that it cannot assess actual practices and the realities of compliance. Any mere inventory of laws or codes would constitute a facile short-cut that does a disservice to the aim of protecting privacy in the 'information society'.

6. The complexity of adequacy assessments documented by this study may also have implications for the use of contracts. The level of detail required for a fair assessment goes beyond many of the contractual schemes currently in development.

7. Our broadest methodological conclusion is that collecting and analysing information about specific transfers of personal data is not a simple task. Assessment of adequacy is not easy or quick to accomplish, nor does it necessarily furnish reliable results. In the future, the process of assessing adequacy will require further refinement of analytical instruments for application to a wider array of transfers and circumstances. The institutional machinery for assessing adequacy and for disseminating results will need careful design.

Practical Difficulties

8. This study proceeded by seeking to identify actual transfers of personal data made by real data controllers or data subjects in Europe to organisations in other countries. In order to describe actual transfers, it was necessary to obtain the co-operation of data controllers in Europe and recipient organisations in destination jurisdictions. Organisations were asked to share with us detailed information about data collection, maintenance, use, and disclosure practices.

9. One problem, therefore, was finding organisations, both in Europe and in third countries, that were willing to co-operate. While the experience varied considerably from organisation to organisation and from country to country, identifying co-operators was generally difficult. However, most organisations consider this information to be proprietary. In addition, they may be reluctant to share potentially embarrassing facts about data processing in an environment of heightened concern about data protection. Because data protection is not a major concern in all of the destination jurisdictions, simply finding a knowledgeable informant who understands the significance of data protection issues is a significant challenge. In some organisations, there is no readily identifiable individual responsible for data protection as broadly defined. We relied at times on trade associations, personal contacts, and other methods to find knowledgeable personnel, but it proved impossible for some recipient organisations.

10. Even when a co-operative individual is found, a more senior official in the organisation may reject the request for assistance. Conversely, in some organisations senior officials may agree to co-operate, but local employees may nevertheless refuse to supply information. In both cases, reasons may include the fear of disclosure, simple disinterest, or a perception of the time and cost involved in co-operating. These are real constraints and require a degree of skill in negotiation to overcome, and this may not be necessarily accomplished in a short time. We had no legal or practical leverage over data controllers and had to rely on good will. In making future assessments, supervisory authorities are likely to secure more rapid and effective co-operation.

11. A further difficulty is identifying a reliable and consistent source of information within an organisation. Since data protection has not so far been a significant issue for many organisations receiving personal data from Europe, formal policies do not always exist and organisational practices are not standardised. Consequently, the same enquiry to the same organisation sometimes produces different answers from different persons, particularly where the implementation of data protection is divided between technical staff and general management. This in itself is an interesting finding about the way data protection is complied with in organisations. Information about some data protection policies and practices is simply unavailable because the co-operating staff member does not know and cannot obtain the information. This may be less of a problem where a local organisation is subject to control by a European parent organisation. However, the inability to obtain information may explain why, in any investigation, one case study may include details that a similar one omits. Information available from one organisation may be unavailable from a nearly identical organisation in another jurisdiction.

12. Another point is that organisations often have many different lines of business that involve the collection and use of personal data. The policies and practices that apply to one line of business may not apply elsewhere in the organisation. This problem is especially likely in large companies with decentralised operational units. While the specific focus of the transfers studied helped to minimise this problem, the lack of a central, co-ordinated policy was apparent in some destination organisations. The result is that a conclusion applicable to one transfer of personal data to one organisation in a destination jurisdiction may not be applicable to another transfer to that same organisation in the same jurisdiction. This will significantly complicate future assessments of adequacy.

13. There are also legal uncertainties surrounding many personal data activities. These come in several different varieties. In some instances, statutes are obscure or have not been authoritatively interpreted. As a result, it is difficult to assess their impact and relevance without extensive legal research and, even then, a definitive conclusion may not be possible. In some jurisdictions, common law offers some prospect of relief to data subjects. However, the common law is often untested, so that the availability of practical relief for data protection matters remains highly uncertain.

14. A further complexity arises from differences in jurisdictions. In the United States, Canada, and Australia, for example, laws afford some protections in one jurisdiction but

not in others. When a recipient organisation operates throughout a federal jurisdiction, the applicability of laws to particular personal data may depend on many factors. It may even be impossible to determine whether the law in a particular state or province is applicable to a data transfer because the storage location for data may not be predictable or because the data are maintained on a computer network accessible at all locations. The issue of jurisdictions is most apparent with Internet transactions. Parties to an Internet transaction may actually have no firm knowledge about the jurisdiction in which other parties exists.

15. Determining whether data protection rules are even applicable to a class of data can be challenging. In some instances, data transfers occur in an anonymised form, with overt identifiers removed. Determining when data have been sufficiently anonymised is difficult because no simple or clear test can be applied. One party to a transfer may consider the data to be anonymous and beyond the scope of data protection, while the other party does not agree. Anonymity sometimes must be evaluated on a scale rather than as an all-or-nothing issue. This is most obvious in relation to certain kinds of data in the health field.

16. Moreover, in many instances it is difficult to distinguish between data transferred from the EU and other data separately collected and held in the third country incident to the transfer. The airline, medical and Human Resources cases illustrate how data with different requirements may blend together in the files of a third-country data controller.

17. An additional problem is that, while the Directive and European Commission documents enumerate the criteria to be taken into consideration in assessing adequacy, there is no clear priority amongst the enumerated items. In most cases, judgements of adequacy must weigh and combine facts that, if taken singly, may point towards different conclusions. There is no mechanical substitute for this judgmental process. It has the advantage of flexibility when used in decision-making contexts that are sensitive in the international relations of data protection. Yet this virtue may have a corresponding vice, that of arbitrariness and the potentiality for disagreements across a range of assessors who are differently positioned and whose ranking of priorities may therefore differ. At that point, measuring adequacy against the privacy risks inherent in certain transfers may be a sensible approach to arbitrating differences. The notion is similar to that of risk assessment for computer security threats. We recognise, however, that this type of assessment may raise further contested issues concerning the nature and analysis of risk that need to be resolved.

18. A final difficulty is that of cultural and institutional non-equivalence. Judgements about adequate protection must remain sensitive to important cultural differences. Despite the growing convergence of international data protection policy, ‘privacy’ still means something very different in various cultural and national traditions, perhaps particularly in non-Western jurisdictions but by no means there alone. Moreover, institutions in different places may perform very different functions and roles, and these differences may not be immediately apparent from their formal description. This problem will be exacerbated as the European Union attempts to apply the adequacy standard in other countries and cultures. This is a classical dilemma of the relationship between international norms and particular circumstances, and it has important consequences for both practical decision-making and analytical investigation.

Compliance Gaps

19. The focus of this study was on the data protection policies that an organisation *reported* to be in place and applicable to its data. Let us recall that Article 25(2) of the Directive draws attention to 'the professional rules and security measures *which are complied with*' in the third country (emphasis added). In some instances, it was independently possible to identify and review the level of compliance with applicable laws or codes of practice. However, we were not empowered to conduct a detailed audit to determine whether an organisation actually complied with the laws and policies applicable to its activities. A full compliance audit requires a major effort as well as extensive access to

an organisation's records and employees. In at least some instances, significant differences appear to exist between policy and practice, but it has not been possible to make any specific assessment of the extent of these discrepancies.

20. The mere existence of an applicable data protection law in a destination jurisdiction is clearly no guarantee of compliance. Laws may have no practical or independent enforcement mechanism, and poor practices may develop in the absence of constant outside pressures. Nor is a determination of compliance at a particular time a guarantee that an organisation will remain in compliance; actual practices may change dramatically over time.

21. Self-regulatory instruments for data protection are highly diverse. Some have been published as privacy codes of practice with the specific hope that they would satisfy the international standards that are found in the OECD Guidelines, the Council of Europe Convention, and the European Union Directive. These are generally the easiest to assess. Others, however, may be buried within guidelines about related issues, such as consumer rights. Others have been clearly devised in order to deflect or pre-empt regulation. In the absence of full compliance audits, it is difficult to distinguish between those self-regulatory instruments that do force some level of compliance, and those that perform little more than a symbolic function. As with law, the mere existence of even a satisfactory code is no guarantee of compliance and the actual protection of privacy.

The Purposes of Assessment and the Role of Assessors

22. This study was performed by a group of independent researchers to assess a methodology. Others will need to undertake similar assessments of adequacy for other purposes. For example, supervisory authorities must assess adequacy when making decisions on the legality of some transfers of personal data. An organisation that wants to transfer data to another country (data exporter) may seek to conduct its own assessment of the recipient organisation. Alternatively, a recipient organisation (data importer) may find it necessary to make its own determination of compliance with international fair information practice standards. In some cases, government agencies other than supervisory authorities might conceivably be authorised to assess adequacy. In addition, privacy advocates may attempt to assess the adequacy of some data recipients in order to use the conclusions for complaints or for critical comment. Finally, it is possible that adequacy determinations could be relevant to litigation over privacy matters, and the determination might become an issue for a judge or even a jury to make.

23. Independent auditors may undertake the same work in some cases, perhaps at the direction of organisations or at the request of supervisory authorities. It remains to be seen if a process for independent adequacy certifications will develop or will be accepted by data protection officials. If so, the process could conceivably mirror the certification of quality standards as it is accomplished today in different countries. Such 'adequacy reporting' might offer standardised and basic information that permits users of the reporting service to make their own judgements about the adequacy of the privacy protection offered by particular organisations. Alternatively, adequacy reporting might just include information that reflects negatively on adequacy or that reflects judgements or formal decisions made by others. Regardless of the exact nature of the reporting, information could be obtained directly from the proposed recipient organisation or perhaps from third parties. Independent adequacy reporting is a largely unexplored notion now, but it may hold promise for the future.

24. Each adequacy assessor is likely to have a different perspective and experience. If an organisation wants to be able to process data originating in the European Union and seeks approval for a transfer from a supervisory authority, the organisation is likely to be much more co-operative. A supervisory authority will have more leverage over such an organisation and will be able to obtain access to more information than would a privacy advocate or an independent consultant. This would certainly be the case if the organisation seeking the adequacy determination bore the burden of proving that its policies complied

with the standards in the Directive. If adequacy is assessed through litigation, a lawyer might even be able to use the discovery process to force disclosures of vast amounts of information that might otherwise be unavailable to other assessors.

25. The value of adequacy determinations by different assessors is likely to vary. Because of the inherent complexity of the task, the lack of any standard methodology, the legal and regulatory uncertainties, and the subjective nature of many judgements, it may not be enough to know the final conclusion of any particular assessment. The identity of the assessor, the methodology employed, and the period for the assessment may be even more important elements than the conclusion. This study, for example, was intended more to illuminate the process of assessment, and its methodology, than to reach a formal yes-or-no conclusion about the adequacy of protection in each case.

26. It may be that the assessment process itself has a beneficial effect on data controllers, regardless of the final conclusion in any instance. This is because the process brings to the forefront issues and questions about practices that would otherwise lie dormant or remain in an unimproved condition. Some organisations recognise that there are broad benefits to be gained from understanding data protection requirements and from using this understanding for improving their practices. Some also find a review of their practices with outside researchers to be highly instructive. This study afforded some organisations specific, if incidental, advice about what types of activities would help to demonstrate compliance with data protection principles. Once the process was complete, several companies reported that the learning experience was valuable. We believe that such organisational learning is important not only for data controllers, but for regulatory and supervisory authorities at all levels. Ways of collecting these experiences, communicating them, and relating them to practical decision-making need to be devised and made part of the normal functions of all those concerned with data protection.

27. In this context, we believe that many problems of compliance monitoring can be alleviated with the use of certifiable privacy standards. When European data protectors, or data exporters, are concerned about transfers of personal data outside Europe, they could insist that the data importer register to a fair information practices standard, a process that would at least require proper self-regulation and regular compliance auditing. Two initial privacy certification schemes have already been introduced in Canada and Japan. These schemes need to be tested for their abilities to provide assurances of adequate data protection in the context of transborder flows of personal data. Ultimately, an international certifiable standard would be desirable, accompanied by a commonly agreed process of conformity assessment that includes the certification of privacy auditors. Existing national and international standards-setting bodies could have an important role in the determination of adequate protection in the years ahead.

Transitional Considerations

28. It will take several years for the European Union Data Protection Directive to be fully implemented. The first few years are likely to be characterised by an evolutionary process, with regular changes, standardisation, and improvements in the process and methodology of assessing adequacy. This study has illuminated some of the questions that will have to be answered during those assessments. Many other questions remain unaddressed and unanswered. These include:

29. will data protection authorities accept an organisation's self-assessment of adequacy, either during the transitional period or otherwise in the future?

30. will a promise or commitment by an organisation to change its policies and practices be sufficient to permit a determination of adequacy, or will independent verification be necessary at stages during the transitional period?

31. are there some practices that may be accepted as sufficient during a transitional period although they may not fully meet the standards in the long run? For example, might an organisation still be assessed as providing adequate protection if it offered data subjects an internal complaint mechanism while developing an independent complaint process?

32. how frequently should positive assessments of adequacy be reviewed? Does the burden of proof change once an initial positive conclusion has been reached or are reassessments subject to the same standards and the same process as the original assessment?

Other Considerations

33. There are a number of other issues that need to be considered. These include:

34. the process that an organisation must follow in order to document or demonstrate adequacy, and the information that decision-makers will require. Would it make a difference if the personal information maintained by the organisation were used for less sensitive activities (e.g., marketing) than for substantive and important decision-making (e.g., credit-granting)? How are the relative risks to privacy to be conceptualised and investigated?

35. the treatment of proprietary or confidential organisational information in the process of assessing adequacy. How will determinations be made and publicised without breaching legitimate organisational interests in confidentiality?

36. the admissibility of complaints about the lack of adequacy or about breaches of fair information practices in third countries. Must a data subject be able to demonstrate harm before a supervisory authority will accept a complaint? Must a data subject be included in the records maintained by the data controller before a complaint about adequacy will be considered? Will complaints from competitors of the data controller be accepted?

37. the 'intelligence capability' for gathering, analysing, and making available information relevant to assessments of adequacy, including assessment of risks involved in the processing of personal data. With what organisations will such responsibilities lie? Are these roles for the Article 29 Working Party, the Article 31 Committee, the European Commission, national supervisory authorities, or independent institutes?

In Conclusion

38. This study was not designed and does not purport to offer broad generalisations about the adequacy of a specific country, organisation, or class of transfers. The conclusions vary considerably between the different categories of transfer and within categories as well. The specific choice of subject-matter for the case studies was pre-determined in the specifications for this Report, and made a considerable difference to the findings. If another study were to select another set of transfers, the conclusions might be significantly different. Indeed, a second study of the same transfers conducted in the next year would likely produce some different conclusions. The reasons for the differences might be changes in practices, different sources of information within organisations, different interpretations of applicable rules, or changes to the laws or to the codes containing those rules.

39. A further problem is that it is not possible to assess adequacy just by reference to the policies and practices of a specific organisation or organisations (there are usually at least two parties to a transfer of data from Europe to a destination jurisdiction). The legal environment in any jurisdiction is always relevant, as is the availability of external oversight, compliance mechanisms, and complaint mechanisms. Looking beyond the

parties to the transfer to this broader regulatory environment is always necessary in any assessment of adequacy.

40. The inventory of questions included in the Appendix provides a systematic basis for assessing the adequacy of privacy protection in third countries and can be applied to a wide range of circumstances and types of data-transfer. However, experience shows that many facts are difficult to ascertain, and that the investigative instrument can only be used effectively where organisations are willing and able to provide answers.

41. There are no shortcuts to the assessment of adequacy. Even the existence of a comprehensive data protection law does not remove the need to ask and answer searching questions. Laws are not self-executing. They require effective supervisory institutions and mechanisms. Codes of practice may have limitations, such as a lack of universal application, exclusion of some principles, as well as weak enforcement and compliance mechanisms. Security measures and privacy-enhancing technologies can offer some protection but cannot provide a complete solution.

42. With the Directive coming into force, there is an urgent need for further refinement of the processes of assessing adequacy in order that different assessors can apply them to a wider array of transfers and circumstances. The stipulated criteria for assessing adequacy are reasonably clear although, as has been mentioned, conceptual problems remain, concerning the meaning of adequacy, sensitivity and risk. The gathering and analysis of the facts faces a number of difficulties, outlined above. What is also needed is the careful design of the institutional machinery for making those assessments, for communicating the results, and for advising assessors, so that better privacy protection can be ensured in the future.

APPENDIX: INVENTORY OF RESEARCH QUESTIONS

This inventory was prepared as a general guide for use in collecting information about the personal-data practices of data controllers who were the subject of this study. It is reproduced here because it might be useful to others who are undertaking similar assessments of adequacy. The questions are not necessarily exhaustive of all issues relevant to adequacy determinations; nor are all questions relevant to each of the transfers studied. In addition, not all the information called for by the questions was available for each case. For each transfer studied, questions from this list were selected as appropriate for the facts of the transfer, and for data controllers in Europe and in the destination jurisdictions. The headings in this inventory correspond to the headings used in each case study.

The Nature and Circumstances of the Transfer

a) What elements of personal data are included in the transfer? Does the transfer include any data deemed sensitive?

b) Why are the data being transferred?

c) Where are the data sent from and where are they received and stored?

d) Who sends the data and who receives the data?

e) How is the data transfer accomplished?

Overview of the Regulatory Environment

a) Are there any comprehensive or sectoral laws about data protection that apply to the transfer? Are there any relevant government regulations about data protection that apply to the transfer?

b) Are there any mandatory sectoral codes of conduct about data protection that apply to the transfer? Are there any voluntary trade association or other industry policies or guidelines about data protection that apply to the transfer?

c) Is there a supervisory authority with responsibility for data protection? Is there a supervisory authority for the industry, activity, or sector that has authority to investigate or review data protection issues?

d) Is there an independent consumer complaint mechanism that accepts and investigates complaints involving data protection?

e) Are there special rules, procedures, or limitations applicable to sensitive data?

f) Are there laws or rules that regulate, authorise, or prohibit the use of automated decision-making?

Purpose limitation, transparency and opposition

a) Are there externally imposed limits on the purpose for which personal data can be collected? How does the data controller describe the limits?

b) What is the source of externally imposed limits:

(i) general or sectoral statutes?
(ii) common law?
(iii) regulation?
(iv) industry code of practice?
(v) formal company policy?
(vi) company practice?

c) Do affiliates, contractors, and agents impose limits on the collection, use, and disclosure of personal data? Have enforcement activities been undertaken?

d) If disclosures to third parties are permitted or required, are there limits imposed on how data may be used and re-disclosed by the third parties? Are there special rules, procedures, or limitations for sensitive data?

e) What are data subjects told about the purpose of collection, and about intended uses and disclosures (notification)?

f) How and when are data subjects told? Is a description or statement publicly available?

(i) Is there a written notice? Is it comprehensive or are there exceptions (stated or unstated)?
(ii) Who is the author of the notice: the controller, the government, or someone else?
(iii) Are notices reviewed or approved by a governmental or other external authority?
(iv) Are notices given or offered to data subjects?
(v) Are data subjects permitted or required to consent to the terms of the notice?
(vi) Can data subjects change their consent later?
(vii) Are notices provided or offered before, during, or after each transaction?
(viii) Is a notice available online?
(ix) Are data subjects permitted or required to make choices about uses or disclosures?
(x) Do limits on use and disclosure cover or bind subsequent recipients of the data?
(xi) Is there a notice about the use of automated decision-making about individuals?

g) What, if any, limits are there on subsequent uses and disclosures not originally specified?

h) In particular, what provision is there for objection or consent to such new uses or disclosures, including but not limited to direct marketing uses?

i) In particular, what provision is there for objection or consent to such new uses or disclosures?

(i) What is the source of any limits? Internal? External?
(ii) Are data subjects permitted or required to agree?
(iii) Do the limits cover or bind subsequent recipients of the data?
(iv) Will data subjects be notified of any later changes?
(v) Can data subjects who are notified of later changes revoke consent or withdraw?
(vi) What are the procedures for revocation of consent?

j) To what extent are personal data accessible to domestic government authorities, and under what conditions?

(i) Are there special legal protections for specific classes of data?
(ii) Is disclosure to a government authority routine or unusual?
(iii) Is a government authority required to have a compulsory process to obtain access? Are data subjects notified of a governmental request?

(iv) Can protections against government access be waived by data subjects or by the controller? If so, how?
(v) Are there limits on the use and further disclosures of personal data obtained by government authorities?

Data quality and proportionality

a) What, if any, limits are there on the data types that can be collected or maintained (either general 'not excessive' limits or specific prohibitions)?

(i) What is the source of the limits?
(ii) Can the limits be waived or modified by the data subject?
(iii) Are any sensitive data collected and, if so, under what conditions?

b) What, if any, requirements are there that data must be accurate, relevant, up to date, and complete?

(i) What is the source of the requirements?
(ii) Are the requirements external, voluntary, or market-driven?
(iii) What is the role of data subjects in meeting the requirements?
(iv) Is there a process that limits the ability of employees to make changes to data without oversight, authority, or controls?

c) Is there a requirement that corrections, updates or other changes be passed on to third-party recipients, including recipients in third countries?

(i) What is the source of the requirement?
(ii) What is the role of data subjects in the process?
(iii) Is consent required before disclosing corrections?

d) What, if any, requirements are there relating to disposal and time limits for retention of data?

(i) What is the source of the requirements?
(ii) Are data subjects notified of the requirements?
(iii) Do data subjects have any choice?
(iv) Do disposal rules apply to records disclosed to affiliates, contractors, and agents?

Security

a) What, if any, requirements are there for appropriate security measures to protect personal data against loss, and against unauthorised access, use, modification, disclosure or destruction?

(i) What is the source of security requirements?
(ii) Does the controller have a dedicated security official?
(iii) Are the security requirements written?
(iv) Are the security rules conveyed to employees? How?
(v) Are employees disciplined if they do not comply with security rules?
(vi) Are there regular security audits? Internal or external?
(vii) Are security measures focused on internal or external security threats?

b) Are there written rules that classify data into different levels of sensitivity?

(i) What is the source of the rules?

(ii) Do the sensitivity levels reflect the definitions in the European Union Directive or are they based on other criteria?
(iii) Do security policies reflect the sensitivity levels in the rules?

c) What, if any, specific security techniques are required or followed - e.g., access control, encryption, audit trails?

(i) Are access controls routinely used to identify wrongful access or wrongful attempts to access data?
(ii) Do audit trails record both internal and external access?
(iii) Are audit trails routinely examined to identify wrongful accesses? How often?
(iv) Is encryption used for data storage, internal transmissions, or external transmissions?
(v) Are there specific policies that govern who has access to encryption keys?

Access and rectification

a) Can individuals obtain access to personal information about themselves, and have corrections made where appropriate?

(i) Are access and correction rights provided as a matter of policy or a matter of law? What is the source of the rights?
(ii) Are procedures clearly defined and time-limited?
(iii) Are data subjects notified of the rights?
(iv) Is access available online?
(v) Is information available that describes the logic used in automatic decision making?

b) What, if any, exemptions or conditions apply to access and correction rights?

1) What is the source of the exemptions?
2) Are data subjects asked to waive their access or correction rights?
3) Do foreign nationals have the same rights of access and correction as citizens?

c) What, if any, costs apply to the exercise of access and correction rights?

d) What, if any, appeal rights and mechanisms are available?

(i) Are appeals handled internally by the controller? Is there an independent review?
(ii) Can or must data subjects appeal through the courts rather than administratively?
(iii) Are alternative dispute resolution mechanisms available?
(iv) Are charges fair and reasonable?

Onward transfer restrictions

a) Are there likely to be onward transfers of personal information to other jurisdiction? If so, are the transfers to other national or local jurisdictions?

b) What, if any, provisions are there for ensuring that protected personal information is either not transferred to jurisdictions where the same protections do not apply, or is only transferred with appropriate safeguards?

1) What is the source of onward transfer restrictions?
2) Are transfer restrictions imposed on the controller's agents, contractors, and affiliates?

c) Are personal data routinely maintained on a computer network that is accessible in other jurisdictions? Do the same data protection rules apply to all jurisdictions from which the data are accessible?

Remedies

a) What, if any, formal mechanism is there for individuals to complain about breaches and to seek redress?

(i) What is the source of the mechanism? Statutory? Regulatory? Company Policy? Trade Association?
(ii) Is the mechanism internal or external to the data controller? Are individuals required to rely on civil courts to find relief?
(iii) Is there an independent source of assistance to individuals who have complaints about fair information practices?
(iv) Is an independent decision-maker available at any point in the complaint process?
(v) Can individuals be awarded specific relief and monetary damages? Are there limitations on the awarding of monetary damages?
(vi) Can criminal penalties apply to controllers?
(vii) Can foreign nationals use the same complaint mechanism as citizens?

b) What, if any, information is made available to individuals about enforcement of their rights?

(i) Is the information provided before data are collected?
(ii) Can individuals obtain a copy of privacy policies on request?
(iii) Are policy documents provided online?

c) Are judicial remedies available to individuals?

(i) Are there statutory remedies or remedies based on common law or contracts?
(ii) Are individuals prevented from seeking relief against sub-contractors of data controllers because of a requirement for privity?
(iii) Can judicial remedies apply to all or just to some of the elements of fair information practices? Can judicial remedies award monetary damages?
(iv) Can foreign nationals use the same judicial remedies as citizens?

Accountability

a) How do record-keepers ensure knowledge of and responsibility for compliance with fair information practices?

(i) Are there written policies and are they disseminated to employees?
(ii) Is there a privacy officer or the equivalent? Is there a security officer or the equivalent?
(iii) Is there an internal mechanism for reviewing policy or for approving new uses and disclosures of personal data?

b) What, if any, requirements are there for regular or periodic internal and external audits?

(i) What is the source of the requirements?
(ii) Are the results of audits made available to the public or to supervisory authorities?
(iii) How regularly are audits for privacy or security conducted?

c) Is there an external supervisory authority? If so, how independent is it and what powers does it have to investigate, award, and enforce remedies?

(i) Is the supervisory authority governmental?
(ii) Can the authority investigate complaints from individuals?
(iii) Can the authority initiate investigations on its own?
(iv) Can the authority impose sanctions on controllers?
(v) Does the supervisory authority offer general assistance to individuals, companies, and trade associations to foster understanding and general compliance?

d) What, if any, requirement for staff training or education about fair information practices is there?

(i) What is the source of the requirement?
(ii) How periodically is training provided?
(iii) Are there professional certification programs?