



COMPUTERS & LAW

NEWSLETTER FOR THE SOCIETIES FOR COMPUTERS
AND THE LAW IN NEW SOUTH WALES, VICTORIA, SOUTH
AUSTRALIA, WESTERN AUSTRALIA, QUEENSLAND
THE AUSTRALIAN CAPITAL TERRITORY AND NEW ZEALAND
Registered by Australia Post - Publication No. NBG 8205

Editors: Elizabeth Broderick, Daniel Hunter
Number 18

ISSN 08117225
March 1992

Implications of the EC Draft Directive on Data Protection for Australia

Graham Greenleaf

International data protection requirements

There is increasing international pressure for data protection laws. Data protection laws of some countries may prohibit the transfer of personal information to other countries which lack adequate data protection laws. The various international data protection agreements, existing and proposed, will not provide protection against restrictions on the transfer of data to or from Australia in the absence of adequate data protection laws covering the private sector. As explained below, the result is that businesses wishing to transfer personal information to or from Australia may be prevented from doing so if Australian law does not provide adequate data protection.

Trans-border data flows (TBDF) of personal information

'Trans-border data flow' simply refers to the movement of data across national borders. In the context of data protection, it only refers to the movement of personal data. How-

ever, TBDF may occur with financial or trade data which does not refer to identifiable individuals, but this TBDF will not raise the same privacy concerns.


Some types of activities which give rise to TBDF privacy concerns include:

1. an international company keeping records concerning citizens of one country in another country;
2. searching databases containing personal information by overseas telecommunications;
3. sending electronic mail overseas; and
4. sending personal data overseas to be processed, for technical or financial reasons, with the intent that the processed data then be re-imported.

In all cases such as these, the country whose citizens are involved may be concerned whether the data will be subject to a proper standard of data protection when it is in the other country. Further concerns may arise if there is a possibility that

it may be exported from that country to a third country. Such concerns have resulted in all European countries with data protection legislation imposing restrictions on TBDF.

In the TBDF context Australia may be the country whose citizens' personal data is being 'exported', or may be the country which is 'importing'

Continued on page 3 

In this issue ... Europe '92

Implications of the EC Draft Directive on Data Protection for Australia	...1
Editors' News	...2
Society News	...9
EC Directive on Product Liability	...14
Total Information Processing Systems Limited v Daman Limited	...17
Book Reviews	...23
Update	...27
Case Note	... 28

From the Editors' Desk

Welcome to the first edition of *Computers & Law* for 1992. In this edition we look at the effect of the changes in the European Community during 1992 on the law of computers.

The EC is currently struggling with all of the problems associated with merging a whole range of disparate cultures, philosophies and laws. The EC bodies charged with this responsibility have created a range of Directives, aimed at integrating the laws of the EC countries. The authors in this edition look at three Directives of relevance to computer lawyers, customers and clients doing business in the EC.

Graham Greenleaf of the University of New South Wales law faculty examines the EC Directive on data protection and privacy. His article examines the various EC responses and the other international conventions in the field. Some of these themes are discussed in a new book by Greg Tucker called 'Information Privacy Law in Australia.' A review of this book is also included in this issue.

Dr Ellen Beerworth of Mallesons Stephen Jaques in Sydney discusses the EC Directive on Product Liability. This Directive is of particular relevance to Australian lawyers since the principles behind it are being imported into the Australian Trade Practices Act. The ramifications for computer manufacturers and importers are serious and wide-ranging. Dr Beerworth examines the Directive and its effect on computer software in particular.

Julian Gyngell, a solicitor with Theodore Goddard in London looks at a recent case decided in England, *Total Information Processing Systems Limited v Daman Limited*. Not only does he examine the decision, but he also discusses the likely outcome were this case or a similar case run pursuant to the EC Directive on the Legal Protection of Computer Programmes. Interestingly, the outcomes of the case under the current law and the EC Directive maybe different. How the English courts will cope with the invasion from the Continent remains a matter for speculation.

Finally, we are delighted to review the first edition of a recently re-launched journal on computer law; the *Journal of Law and Information Science*. The *Journal*, the only academic journal on the subject in Australia, is extremely informative and promises to cover subjects in the field in far greater detail than this humble broadsheet can hope to aspire to. We wish the editorial board every success and hope to work closely with them in future.

The Editors

As you can see the newsletter has taken on a new look for 1992. We have dispensed with the rather drab brown and yellow colour scheme and replaced it with colours more suited to the informative and interesting publication it now is.

Whilst the colours have changed the quality of the content has not and we believe the 1992 editions of *Computers & Law Newsletter* will be highly regarded!

Virginia Gore

Computers & the Law

Editors

Elizabeth Broderick
cl- Blake Dawson Waldron
Grosvenor Place, 225 George Street
SYDNEY 2000

Daniel Hunter
cl- Tolhurst Druce & Emmerson
389 Lonsdale Street
MELBOURNE 3000

Layout & Design

Virginia Gore

Subscriptions: \$32.00 per 4 issues.

Advertisements: Inserts \$300.00; For advertisements within the newsletter, rates and information will be provided by the Editors on request

Articles, news items, books for review and other items of interest may be sent to the editors.

Newsletter contents may be reproduced if the source is acknowledged.

 Continued from page 1

personal data concerning citizens of another country. Examples of TBDF which are relevant to Australia could include:

1. the computer of a credit bureau, located in Australia, which contains the credit files of its associated New Zealand company, so that New Zealand credit grantors obtain credit reports via the Sydney computer;
2. international credit card companies may store and process cardholder details in countries other than that of the card-holder;
3. international electronic mail services which are used by many Australians;
4. database systems in Australia which overseas users may search; and
5. electronic document interchange (EDI). EDI is becoming of increasing importance to Australian businesses, and though it will not usually involve personal data it may do so.

A number of world-wide data transmission networks exist, such as SWIFT (Society of Worldwide Interbank Financial Telecommunications) for financial transactions, and SITA (Societe Internationale des Telecommunications Aeronautiques) for travel reservations and airfreight and flight information. Both these networks, and the others which will develop, raise TBDF considerations.

The rapid increase in the importance of trade in information services has given rise to a separate set of concerns regarding TBDF. Many concerns have been expressed that data protection laws could easily be used as an excuse for what are, in effect, non-tariff trade barriers. Mas-

querading as data protection laws, these would actually be designed to keep the economic benefits of data processing activity within the boundaries of countries whose citizens are the subject matter of the data.

It is this apparent conflict between the equally legitimate goals of data protection and that of free trade in information services which has, in significant part, led to a search for international solutions. To date, the solutions have been in the form of

"All European data protection Acts contain provisions by which their national data protection agency has authority to restrict 'exports' of personal data"

the *OECD Guidelines*, the *Council of Europe Convention*, and now the European Commission draft Directive, all of which address the problem specifically.

TBDF restrictions in national laws

All European data protection Acts contain provisions by which their national data protection agency² has authority to restrict 'exports' of personal data. The enforcement of such prohibitions may become mandatory if the European Commission draft Directive is adopted. For example, s12 of the United Kingdom *Data Protection Act 1984* provides that where data is to be transferred to a State which is not a party to the

European Convention,³ the Registrar may issue a transfer prohibition notice provided certain criteria are met. The Registrar must be satisfied that the transfer is likely to lead to a contravention of the data protection principles in the United Kingdom Act because the other country does not have adequate data protection laws. The Registrar cannot prevent the transfer of personal data to any State which is bound by the *Council of Europe Convention* unless he is satisfied that it is intended to be transferred to another country where there is likely to be a contravention of the data protection principles. The UK Data Protection Registrar issued the first Transfer Prohibition Notice in December 1990, prohibiting the export of personal data to a mail order company which operated from the United States. There was evidence that the company had breached UK consumer protection laws, and had been prosecuted under similar US laws.

Some countries go further, specifying that an 'export licence' must be obtained for the exporting of any personal data coming within the legislation,⁴ or that a licence must be obtained for specified categories of personal data.⁵ A few countries also require licences for the import of personal data, not merely compliance with national laws.

The OECD Guidelines and TBDF

In 1980 the Council of the OECD made a Recommendation⁶ that, inter alia, its member countries "take into account in their domestic legislation" a set of principles contained in *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* annexed to the Recommendation. In 1984 Australia announced its intention to adhere to the *Guidelines*. The

Preamble to the *Privacy Act* recites that "Australia has informed that Organisation that it will participate in the recommendation concerning those Guidelines." The OECD *Guidelines* are the only international privacy instrument to which Australia is a party.

The OECD's *Guidelines* contain four basic principles of international application concerning the free flow of, and legitimate restrictions on, TBDF.⁷ In 1985 the Ministers of the OECD Member countries adopted a Declaration on *Transborder Data Flows* agreeing to undertake further joint work on TBDF issues.

The main thrust of these OECD principles is that member countries should avoid restrictions on the free flow of personal data between themselves, with three exceptions in Guideline 17. The first exception in Guideline 17 is where the other member country "does not yet substantially observe these Guidelines," including the Principles of domestic application. The OECD *Guidelines* apply to both the public and private sectors.

The *Privacy Act 1988* (Cth) substantially implements the *Guidelines* in respect of the Commonwealth public sector, and was enacted partly so that Australia can comply with its announced adherence to the *Guidelines*. Several state *Freedom of Information Acts* implement some of the *Guidelines* in relation to the public sectors of some States.

However, the *Guidelines* do not provide protection against the imposition of TBDF restrictions by other OECD countries against Australia. No Australian legislation yet requires the private sector to comply with the *Guidelines* generally. The Commonwealth credit reporting legislation (*Privacy Amendment Act 1990*) may constitute compliance insofar

The OECD's 4 Principles concerning trans-border data flows

15. Member countries shall take into consideration the implications for other Member countries of domestic processing and re-export of personal data.
16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country are uninterrupted and secure.
17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other member country provides no equivalent protection.
18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection."

as consumer credit information is concerned. It is therefore possible for other OECD member countries to refuse to allow transfers of most categories of private sector personal data between it and Australia, without that country breaching the OECD *Guidelines*.

The requirement in Guideline 15 that trans-border data flows "including transit through a Member country, are uninterrupted and secure" may be addressed in part by such legislation as the *Telecommunications (Interception) Act 1979*.

Neither the *Privacy Act* nor other Australian legislation imposes any special restrictions on the import of personal data into Australia or the export of personal data from Australia.

The Council of Europe Convention and TBDF

The Council of Europe Convention, Chapter III, contains provisions with similar intent to those in the OECD *Guidelines*, but which define the obligations of the contracting parties more carefully. The principal provision, subject to certain exceptions, provides that "a Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another party." The principal effect of such provisions is to protect contracting States against other contracting States imposing restrictions on the transfer of personal data to or from them, except in carefully limited circumstances. Countries such as Australia which are not parties to the Convention have no protection against the imposition of such restrictions. Most European States have imposed such restrictions.

It is possible for Australia to accede to the Convention, if invited to do so by the Council of Europe. Australia has not sought to so accede.

The European Commission draft Directive

The most significant international pressure for increased data protection in the Australian private sector

is likely to come from the proposal by the Commission of European Communities for an EC Council Data Protection Directive. The Commission's draft Directive, issued in September 1990,⁸ is proposed to take effect on 1 January 1993. The Directive will be considered by the European Parliament. In early 1992 the Presidency of the EC will attempt to harmonise the recommendation of the Parliament and the Council's own expert group. A new draft will then be resubmitted to Parliament before being placed before the Council for adoption sometime in 1992.

The EC Directive and TBDF

Neither the OECD *Guidelines* nor the Council of Europe Convention *require* their signatories to impose TBDF restrictions on non-signatory countries, or on countries which do not provide an equivalent degree of protection. They do not contain any positive requirement to restrict exports, but leave this up to the signatory countries. This is where the EC Draft Directive provides a stark contrast, because it makes it mandatory for EC countries to prohibit the export of personal data to any countries (such as Australia) which do not provide "an adequate level of protection."

Chapter VIII of the draft Directive provides that "The Member States shall provide in their law that the transfer to a third country, whether temporary or permanent, of personal data which are undergoing processing or which have been gathered with a view to processing may take place only if that country ensures an adequate level of protection."

Main elements of the EC draft Directive

The Directive applies to personal data held in private sector commer-

cial files and public sector files, except public sector files concerning activities falling outside Community law. Non-computerised data is covered so long as it is "structured and accessible in an organised collection."

In relation to private sector files, the key rules are:

1. Processing of personal data (including collecting and recording it, and communicating it) is unlawful without the consent of the data subject, subject to three exceptions.⁹ Consent is only valid

"Non-computerised data is covered so long as it is 'structured and accessible in an organised collection' "

if the data subject receives prior notification of the purposes of collection and any proposed recipients, and may be withdrawn prospectively.¹⁰

Processing without consent is only allowed if:¹¹

- (a) it is carried out under a contract, "or in the context of a quasi-contractual relationship of trust"¹² with the data subject, and is necessary for its discharge; or
- (b) the data comes from generally accessible public sources and is used for 'correspondence purposes' only;¹³ or
- (c) the processing is for the file controller's 'legitimate in-

terest,' which 'prevails'¹⁴ the interest of the data subject.

2. Personal data can only be used for the purpose for which it was collected,¹⁵ and can only be communicated to third parties for purposes 'compatible' with that purpose,¹⁶ although the wording of these provisions is not altogether clear. This is the principle of 'finality' - that use and disclosure are limited to the original purposes of collection.

Slightly less stringent rules apply to private sector files, particularly in relation to the sharing of data between government agencies,¹⁷ but submissions have been made to the EC¹⁸ that the same rules should apply.

3. Data subjects are to be given further rights in relation to both public and private sector files,¹⁹ including rights:
 - (a) Not to be subject to decisions reached by purely automated means. For example, an automated credit scoring system would be illegal unless a final human decision was involved similarly for the granting of a pension, or the issuing of a tax assessment.
 - (b) The usual rights to know of the existence of files, to obtain a copy of their own file, and to obtain corrections.
 - (c) To obtain erasure of data used for market research or advertising
 - (d) To oppose any wrongful processing, and to have a 'judicial remedy.'
4. The types of files kept by private and public sector bodies must be notified to the national data pro-

Your authoritative guide to the new EC Directive is right here ...

Legal Protection of Computer Programs in Europe

by Czarnota and Hart

The legal protection of computer programs is one of the most important issues identified by the Commission of European Communities. That's why the EC's Directive on legal software protection was adopted in May 1991.

But just how do you interpret the Directive? And where do you go to get a practitioner's view on how to deal with the issues raised for the industry and the legal profession?

Legal Protection of Computer Programs in Europe by Butterworths answers these questions and more.

This book is designed to provide you with:

- an authoritative history and interpretation of the Directive, as well as
- an international perspective, including a valuable comparison of the EC Directive with the law of the US, Japan and Eastern Europe

If you're a legal adviser to software developers and distributors, or even involved in the drafting of licences in the software industry, you must own a copy of this indispensable book.

Butterworths UK 1991 Hardcover 0 406 00542 7 \$215.00 rrp

For more information on this and other titles, please contact Diana Minglis at Butterworths on (02) 335 4452

Butterworths Pty Limited ACN 001 002 357, PO Box 345, North Ryde NSW 2113

Butterworths 

tection Commissioner, so that a national register can be kept, but only where data is intended to be disclosed to third parties.²⁰ This need not be a licensing system.

Most of the other 33 Articles provide additional rights and liabilities, including security measures,²¹ the requirement that a national data protection authority have investigative powers and rights of access to files.²² These are merely some key provisions.

What can constitute an 'adequate level of protection?'

There are two methods by which exports of personal data from the EC will be legal.

First, the laws of a country such as Australia may be determined to provide an 'adequate level of protection' when considered in their entirety.²³ It seems that such determinations will occur in a piecemeal way. The Commission may decide that an importing country has an adequate level of protection "by reason of the international commitments it has entered into or of its domestic law."²⁴ It is a matter of speculation whether the Commission will declare some countries to have such protection from the outset.

Where doubt exists, the EC Commission must be informed by a Member State of any importing third country to which it proposes to export personal data which does not have an adequate level of protection. The Commission may then enter negotiations with that country "with a view to remedying the situation." Unless the Commission then makes a decision that the country concerned does have an adequate level of protection, any export of personal data to that country would

constitute a breach of the Directive by the EC country concerned.

The EC Commission is reported to prefer an approach whereby non-EC countries would accede to the Council of Europe Convention and ratify their accession after passing laws 'equivalent' to the Convention.²⁵ The EC Commission would then declare that the country had 'adequate' laws, and it would be bound under international law by the Convention.

Second, where a country's overall laws do not provide adequate protection, it is possible for a particular data export to be legal.²⁶ The controller of the file from which data is

"There are two methods by which exports of personal data from the EC will be legal"

to be exported may submit to the designated national authority in the EC Member State evidence that adequate protection will be provided in this particular case. The Member State may grant an exception,²⁷ but only after it has informed the EC Commission and neither the Commission nor another Member State has objected within 10 days. If such objection is raised, the Explanatory Memorandum²⁸ says the EC Commission can take appropriate measures, including prohibition of the transfer.

'Adequate level of protection' is not defined in the draft, and the Explanatory Memorandum simply says that it is "for the Member States, and if necessary for the Commission, to determine".

Some of the questions which will need to be raised include:

1. Need there be adequate compliance with each EC requirement, or just most of them? The use of 'adequate' may suggest that only some partial compliance is required. However, there are submissions to the EC29 that 'adequate protection' should be replaced with 'equivalent protection',³⁰ thereby strengthening the requirement even further.
2. Can private contracts between data suppliers and recipients constitute adequate protection? The US government is pushing such an approach,³¹ and the French data protection authority, CNIL, has allowed a number of transfers from France to countries without data protection laws on condition that such contracts were entered into.³² The International Chamber of Commerce (ICC) is also promoting such an approach and has prepared a model contract.³³ However, such an approach has considerable problems, as there would be no privity of contract with the data subject, and therefore no enforceable legal rights necessary to satisfy.³⁴ It is also difficult to see how individuals could afford to pursue any rights they were given, if the only remedy were to sue a large corporation, possibly in a foreign country.
3. Can industry self-regulation through codes of conduct constitute adequate protection? Article 20 requires Member States to encourage the development of European codes of conduct, on the basis of the principles of the Directive, but the EC Commission does not regard these as a substitute for legally binding pro-

visions, merely an elaboration of such provisions.

For the same reasons as stated in relation to private contracts, voluntary codes of conduct are also unlikely to constitute adequate protection, although it is possible that a scheme run by an industry body which was shown to have enforcement powers might be sufficient. A code backed up by legally binding enforcement procedures may well constitute adequate compliance.

Does Australia have an 'adequate level of protection?'

Aspects of our general law, such as breach of confidence, negligent misrepresentation or computer crime laws, provide a patchwork of privacy protection falling well short of the EC standards. The two State laws creating Privacy Committees (NSW and Queensland) do not create any enforceable right of privacy and are not 'adequate.'

The *Privacy Act 1988* is likely to satisfy most of the requirements of the draft Directive insofar as the receipt of personal data by the Commonwealth Government and overseas governments (or companies), although a detailed analysis is still required. This will be important in such areas as police and immigration information.

It is unlikely that any State government could claim that, even if it does have a *Freedom of Information Act*, it provides adequate protection for State public sector data. However, as State governments receive a more limited amount of personal data from overseas, this is unlikely to present a major problem except in relation to police information.

Australian law would be unlikely to satisfy the EC requirements in rela-

tion to the private sector, except in relation to credit reporting information. The *Privacy Act* coverage of credit-reporting is certain to provide an adequate level of protection in relation to most of the EC's requirements. This would still require consent to data transfers from the EC to be obtained on a case-by-case basis under Article 25.

Australia's adoption of the OECD *Guidelines* in 1984, although relevant to the EC Commission's decision under Article 24, is unlikely to mean that we have adequate protection. The *Guidelines* have remained largely unimplemented in relation to the private sector for seven years since Australia 'adopted' them.²

Graham Greenleaf is a Senior Lecturer, Faculty of Law, University of New South Wales

Footnotes

¹ This article is an extract from a paper delivered at the December Gala Seminar of the New South Wales Society for Computers and the Law, 4 December 1991

² Equivalent to the Australian Privacy Commissioner

³ For example, Australia

⁴ Iceland and Luxembourg

⁵ Austria, Denmark, and Sweden

⁶ Dated 23 September 1980, contained in *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* OECD, Paris, 1981

⁷ Principles 15-18

⁸ Com(90) 314 final - Syn 287

⁹ Article 8.1

¹⁰ Article 12

¹¹ Article 8.1

¹² For example, a doctor or lawyer,

¹³ That is, an exception for direct marketing, which is to be the subject of a separate Commission directive

¹⁴ Outweighs?

¹⁵ Article 16

¹⁶ Article 8.2

¹⁷ Articles 5 and 6

¹⁸ For example by the Data Protection Commissioners

¹⁹ Article 14

²⁰ Articles 7 and 11

²¹ Article 18

²² Article 26

²³ Article 24

²⁴ Article 24.4

²⁵ *Privacy Laws & Business*, October 1990, p6

²⁶ Article 25

²⁷ Termed a 'derogation'

²⁸ But not the draft Directive

²⁹ For example, by the European Data Protection Commissioners

³⁰ That is, equivalent to the EC Directive

³¹ TDR, Sep/Oct 1991, p37

³² 65 ALJ 560

³³ *Privacy Laws and Business*, October 1991, p6

³⁴ Article 14

Contributions

for

June 1992 Issue

Theme: Intellectual Property

The theme for this issue will be Intellectual Property.

Please send all articles, news items, books for review and other contributions for this issue to the editors no later than 12 June 1992.

