A QUESTION OF ADEQUACY? THE EUROPEAN UNION'S APPROACH TO ASSESSING THE *PRIVACY AMENDMENT (PRIVATE SECTOR) ACT 2000* (CTH)

ANEURIN HUGHES*

I INTRODUCTION

The continuing information revolution is increasing exponentially the capacity to collect and process vast quantities of personal information. At the same time, globalisation means that businesses increasingly want to transfer data from one legal jurisdiction to another. The need, therefore, for appropriate mechanisms to protect the fundamental human right to privacy, while allowing the legitimate use of and trade in data, has never been greater.

II THE PROTECTION OF PERSONAL DATA WITHIN THE EU

For this reason, the European Union ('EU') adopted the 1995 Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[1] This Directive harmonises Member States' data protection laws – with a view to ensuring the free movement of personal data within the EU – while also ensuring that the privacy of individuals enjoys a high level of protection. The Directive is thus a natural and necessary consequence of the European single market. Without it, different national approaches to data protection would create barriers within the market, and the free movement of personal information would be impaired.

The Directive is a framework instrument, establishing basic principles that are applicable to all types of personally identifiable data, regardless of the means by which the data is processed. It places obligations on those who collect, process or transfer personal data, and accords rights to data subjects.

As of March 2001, eleven Member States had implemented provisions into national law. The European Commission ('the Commission') has initiated

---

* Head of Delegation, Delegation of the European Commission to Australia and New Zealand.

1 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995. The full text of the Directive is available at <http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html> at 5 June 2001.

proceedings before the European Court of Justice against the remaining Member States (France, Germany, Luxembourg and Ireland) for failure to comply with the obligation to transpose the Directive's requirements into their national legislation by 25 October 1998.

III TRANSFER OF DATA TO NON-EU COUNTRIES

The Directive also establishes rules designed to ensure that data is only transferred to non-EU countries when there is an adequate (and continued) level of protection, or when certain specific exemptions apply (under arts 25 and 26 of the Directive). Without such rules, which are in full compliance with the World Trade Organisation's General Agreement on Trade in Services ('GATS'), the high standards of data protection established by the Directive would be quickly undermined, given the ease with which data can be exchanged between countries using international information networks.

The Directive provides for the blocking of specific transfers where necessary, but this is a solution of last resort, and there are several other ways of ensuring that data continues to be adequately protected while not causing disruption to international data flows and the commercial transactions with which they are associated (principally through art 26, which allows, for example, for specific contractual provisions and the giving of consent).

IV THE PROCESS FOR ASSESSING ADEQUACY

In implementing the Directive, the Commission is assisted by a Committee and a Working Party. The Committee, set up by art 31 of the Directive, is composed of Member State officials, with every Member State represented. Its particular task is to advise the Commission on decisions concerning the adequacy of the protection of individuals with regard to the processing of personal data for the purpose of transferring it to non-EU countries. The Working Party, established under art 29, is composed of the data protection commissioners, or independent supervisory authorities, of all the Member States. Its remit is wider than that of the Committee; in particular, it plays an important role in helping the Commission to ensure the even application of the Directive's requirements across the EU.

The EU Council of Ministers and the European Parliament have granted the Commission the power to determine, on the basis of art 25.6, whether a non-EU country ensures an adequate level of protection by reason either of its domestic law or of the international commitments it has entered into. Following the advice of the Working Party, the Commission has recognised that an adequate level of protection could also be provided by sector specific legislation or effective self-regulatory schemes (for example, schemes whose enforcement is underpinned by law).

The adoption of a Commission decision based on art 25.6 of the Directive involves firstly a proposal from the Commission, then an opinion by the Working Party (which is non-binding), and finally an opinion by the Committee (delivered by a qualified majority of Member States). The European Parliament then has a 30-day period within which to exercise its right of scrutiny – to check whether the Commission has correctly used its executing powers – before the Commission formally adopts its decision.[2]

However, in the case of Australia, the Working Party considered the Australian legislation in advance of the Commission making a proposal. Its recently issued Opinion therefore provides early input into the process of determining adequacy.

The effect of a positive Commission decision on adequacy is that data can flow freely between the EU and a third country without any further safeguards being required. The Commission has so far made determinations to recognise Switzerland, Hungary and the United States Department of Commerce's 'Safe Harbor' agreement as providing adequate protection.[3]

V THE ADEQUACY OF PROTECTION IN AUSTRALIA

On 26 March 2001, the Article 29 Working Party released its Opinion on the adequacy of the *Privacy Amendment (Private Sector) Act 2000* (Cth) ('the Act').[4] It welcomed the adoption of the Act, and the innovative value of the co-regulatory scheme it introduces. The Working Party nevertheless noted a number of areas of concern in relation to the Act, and therefore advised that data transfers to Australia could be regarded as adequate *only* if appropriate safeguards were introduced to meet these concerns. This could be achieved either on a case-by-case basis (through the adoption of voluntary codes of conduct, foreseen by Part III of the Act), or by a change in the law.

Eight areas of concern were identified in the Working Party's Opinion on the Act, which are similar to those highlighted in the Commission's own submission to the federal House of Representative's inquiry into the then Bill.[5]

1 *Small Businesses and Employee Data Generally*

The first concern relates to the exclusion from the Act of small businesses and employee data. Obviously, if a sector is excluded from the Act, any adequacy

---

2 In accordance with the 'comitology rules' contained in Council Decision 1999/468/EC of 28 June 1999, laying down the procedures for the exercise of implementing powers conferred on the Commission.

3 Further information on the EU's approach to data protection is available at <http://europa.eu.int/comm/internal_market/en/dataprot> at 5 June 2001. Note that the Commission has not made any negative determinations to date.

4 The full text of the Article 29 Working Party's Opinion (Opinion 3/2001) is available at <http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp40en.pdf> at 5 June 2001.

5 The full text of the Commission's submission to the House of Representatives Committee on Legal and Constitutional Affairs regarding its inquiry into the Privacy Amendment (Private Sector) Bill 2000 (Cth) is available at <http://www.aph.gov.au/house/committee/laca/Privacybill/sub113.pdf> at 5 June 2001.

finding on the legislation must also exclude the sector. Yet the importance of these two sectors means that their exclusion undermines the integrity of the legislation when considered from the point of view of trade in data.

For small businesses, only those deemed to pose a 'high risk' to privacy are covered by the Act (although, as a result of amendments, other small businesses can voluntarily choose to opt in, with the Federal Privacy Commissioner keeping a register of such businesses). Setting aside this 'opt in' possibility, when viewed from overseas, the complexity of the small business exemption makes it very difficult to determine (a) which Australian businesses are small businesses, especially over the Internet, and (b) whether or not they are exempt from the Act. From an EU Member State privacy commissioner's perspective, this uncertainty renders it necessary to assume that all data transfers to Australian businesses are *potentially* to small business operators who are not subject to the Act, unless the name of the business is included in the Australian Federal Privacy Commissioner's Register.

The general employee data exemption is of particular concern; based on experience with the United States ('US') (and there is no reason to expect Australia would be different), the most common form of data traded is human resource data. Such data often contains sensitive information and the Working Party could see no reason, in its opinion, for excluding employee data from the provisions of the Act which protect sensitive data. Moreover, the exemptions allow information about previous employees to be collected and disclosed to a third party (for example, a future employer) without the employee being informed. In the Working Party's opinion, the risk of privacy violations makes it all the more important to impose additional safeguards when exporting this type of data to Australia, and the Working Party has recommended that EU operators put into place appropriate additional protection, for example, through contractual clauses.

2 *Exceptions 'Authorised by Law'*

The second concern relates to the exception from the requirements of the substantive data protection principles in the Act where disclosure is authorised by law.[6] According to the Working Party, it is acceptable for there to be an exception when organisations are faced with conflicting legal obligations, but to widen the exception to cover all options offered by sector specific laws, past, present and future, risks undermining legal certainty and virtually defeating the 'purpose limitation principle' found in the Act (which requires an organisation not to use or disclose personal information for a purpose other than the primary purpose for which the information was collected).

3 *Publicly Available Data*

The third concern relates to publicly available data. Under the Act, once data that has been collected is compiled in a form that falls within the definition of a 'generally available publication' all individual rights in relation to that data

6 See National Privacy Principle 2.1(g).

(such as access and correction) are excluded. Further, the Working Party was particularly concerned at the lack of protection for secondary uses of such data, since there is no such general exemption in the 1980 Organisation for Economic Co-operation and Development ('OECD') *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, and such an approach is contrary to that adopted in the EU Directive.

4 *Transparency in Data Collection*

The fourth concern relates to transparency on the part of organisations when data is collected from individuals. Although the Act provides that, normally, organisations must inform individuals of the purpose for which personal data is collected either before or at the time of collection, the Act also permits organisations to inform individuals 'as soon as practicable' thereafter.[7] This is contrary to the accepted international benchmark,[8] and is of particular concern with regard to sensitive data, where the giving of consent by the individual is one of the limited situations in which collection of such data is permitted.

5 *Use of Data for Direct Marketing*

The fifth concern relates to the collection and use of data for direct marketing and the ability of individuals to opt out of such collection. The Working Party had previously given an Opinion on this aspect when considering the generic conditions for the transfer of personal data to non-EU countries.[9] It determined that allowing personal data to be used for direct marketing without an opt out approach being adopted cannot, in any circumstances, be considered as adequately protecting an individual's privacy. Yet under the Act, it is not necessary to give an individual the opportunity to opt out in order to use personal data for direct marketing, provided that direct marketing was the primary purpose of collection. This exemption is of particular concern since (a) data can be collected from third parties and (b) publicly available data is not protected at all. The exception is all the more incomprehensible when direct marketing is the secondary purpose of collection; in such cases, the opportunity to opt out must be given every time the organisation contacts the individual.

6 *Treatment of Sensitive Data*

The sixth concern relates to the treatment of sensitive data: the Act allows most sensitive information which has been collected for a 'legitimate' purpose to be used for other purposes, subject only to the normal restrictions that apply to all types of data. This is a weaker protection than is available in the EU, where it is forbidden to process (ie, collect, use and disclose) sensitive data unless one of a number of specific exemptions is applicable.

---

7 See National Privacy Principle 1.3.

8 Organisation for Economic Co-operation and Development, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (1980) Principle 9.

9 The full text of the Article 29 Working Party's Opinion (Opinion WP12) is available at <http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp12en.pdf> at 5 June 2001.

7 *Lack of Correction Rights for EU Citizens*

The seventh concern noted by the Working Party relates to the lack of correction rights for EU citizens. Under the Act, access and correction rights are limited to Australian citizens and permanent residents. As a result, EU citizens who do not hold this status, but whose data is transferred from the EU to Australia, are deprived of these rights.

8 *Onward Transfer of Data*

The eighth and final concern of the Working Party is in relation to the onward transfer of data from Australia to other non-EU countries. The extraterritorial operation of the Act specifically applies only to Australians and does not extend the protection to non-Australians. This means that, for example, an Australian company could import data from or about European citizens, and then export it to a country with no privacy laws without the Act applying. Such a measure would therefore make it possible to circumvent the EU Directive, should Australia be recognised as providing adequate protection.

VI AUSTRALIA'S LEGISLATION VERSUS THE UNITED STATES' 'SAFE HARBOR' AGREEMENT

Some have argued that to make a positive finding of adequacy in relation to the US 'Safe Harbor' mechanism but not in relation to Australia's legislation is inconsistent. Such criticism is misplaced. Each adequacy finding entails an in-depth analysis, including the commissioning of studies of the specific provisions relating to the protection of personal data in the country being assessed. The assessment considers all relevant aspects, taking into account both the content of the provisions and their enforcement. While a minimum set of criteria is always used to ensure a common approach, and constant reference is made to the OECD Guidelines, the specificity of the country's overall system is also taken into account. Thus a shortcoming in one country need not be automatically acceptable in another. Otherwise, the standard would become the sum of all the shortcomings or exceptions to data protection principles present in third countries.

As far as enforcement of the rules established by the Directive is concerned, the Australian situation is *a priori* better than the US position, in so far as it already includes the infrastructure needed to accompany legal protection of privacy (for example, direct recourse for individuals to the courts and a Federal Privacy Commissioner to oversee implementation). Yet as regards the substance of the legal protection offered, it falls short of the 'Safe Harbor' standard in several ways, specifically in relation to rights of access and correction, onward transfer, direct marketing, derogations and the general scope of the protection.

For these reasons, the Australian case will be examined by the Commission on its merits alone, by reference to established OECD benchmarks and in accordance with GATS commitments.

VII WHERE TO FROM HERE?

The Working Party's Opinion is an independent advisory report and so does not mark the end of the process. At this point in time, the European Commission will not be issuing a decision on the adequacy of the *Privacy Amendment (Private Sector) Act 2000* (Cth).

The Commission has been engaged in a dialogue with the relevant Australian authorities for the last year on this issue and is ready to continue these discussions with a view to finding a solution which would allow a positive adequacy determination to be made in the future, thereby facilitating the trade in data between the EU and Australia.

In the interim, the EU Directive has enough flexibility to allow data to continue to flow unhindered between the EU and Australia, *provided that* adequate safeguards are put into place in the form of contractual agreements or approved industry codes.