February 1999

Testing the adequacy of privacy protection: How will the EU enforce its directive?

Jay Forder

Bond University, jay_forder@bond.edu.au

Follow this and additional works at: http://epublications.bond.edu.au/law_pubs

Recommended Citation
Jay Forder. (1999) "Testing the adequacy of privacy protection: How will the EU enforce its directive?" .

Testing the adequacy of privacy protection
How will the EU enforce its directive?

by Jay Forder, Consultant Editor

Introduction
The European Union's privacy directive adopts high standards regarding the protection of personal data. Article 25 effectively requires its trading partners to do the same. With many countries unable to match these standards, there has been much speculation about how and when the EU will enforce these requirements.

At the close of 1998, the EU released an interesting final report. It received little publicity but indicates the EU is taking tentative steps towards enforcing the directive. It also highlights the difficulties involved.

The report is titled "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". It was produced by the University of Edinburgh and compiled by four international experts in privacy law: Charles Raab, Colin Bennett, Robert Gellman and Nigel Waters.

Six countries were selected for the tests: Australia, Canada, China (Hong Kong), Japan, New Zealand and the United States of America. In each case, the transfer of five categories of personal data were studied and conclusions drawn, not only about the adequacy of the protection but also about the assessment methodology.

The authors appear to have based their review on actual or typical data transfers, supplemented with hypothetical facts. Confidentiality is respected by the use of fictitious names. This article will summarise each of the reviewed transfers to Australia.

Transfer of human resources data
The first scenario involves an employee of a European bank being seconded to work in Brisbane for an Australian bank that is part of the same group of banks. The Brisbane bank's human resources office receives information about the employee from the European bank and directly from the employee.

As part of an international group, the Brisbane bank has a world-wide internal "code of conduct". Largely as a result of this, the review concludes that many elements of fair information practices have been accepted by the bank. It concludes that the bank is also committed 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 Australian Banking Association and Australian Direct Marketing Association's plans to adopt the Privacy Commissioner's National Principles are implemented".

However, the report notes that these commitments relate to customer personal information. It is unclear whether the National Principles will extend to personnel records.

My scorecard: This might just be a passing grade because of the bank's own standards.

Sensitive data in airline reservations
The second scenario reviews the transfer of data when a citizen of an EU member country travels by air to Australia. The citizen needs a wheelchair and kosher meals. This data is recorded as internationally recognised IATA codes. The passenger also provides information for an electronic visa application.

While there is no airline industry association proposing to adopt the Australian National Principles, the report notes that airlines will be affected by the planned Victorian legislation if data is held or used there. The International Civil Aviation Authority's Code of Conduct says that airlines are "responsible for safeguarding the privacy of personal data", but it has no enforcement powers.

The report concludes that, while information is held by an airline, the potential for privacy breaches is quite limited because of the integrity and security of airline systems. Once the data leaves the control of the airline (passing to local agents or third parties), "there is no statutory 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."

My scorecard: Probably a failing grade.

Medical data
The third scenario contemplates an EU citizen travelling in Australia and being taken to a public hospital in Canberra after being found unconscious. A card in her possession indicates she is a diabetic and provides a telephone number in the EU country. A doctor in Canberra contacts her doctor and obtains information about her.

In this situation, apart from a few minor provisions, the Health Records (Privacy and Access) Act 1997 (ACT) "appears to contain major privacy principles and accountability mechanisms equivalent to those set out in the EU Directive". But this stands out as the exception – none of the other States or Territories has equivalent legislation – and the report concludes that health privacy protection in Australia is very uneven.

My scorecard: OK in ACT, but a failing grade elsewhere.

Electronic commerce data
The fourth scenario describes an Australian retailer and mail-order company in outer Sydney. It does an increasing volume of business through its web site using NetCommerce, a proprietary Internet shopping product. European customers transfer data about themselves to the retailer, often including credit card details through an encrypted link.
There is an argument (provisionally adopted by the EU’s Data Protection Working Party) that the web site publishers are “processing” personal data on the web user's equipment, and are therefore subject to the data protection laws of the user’s country (ie the EU). The report specifically disregards this argument and concentrates on privacy protection in the country hosting the web site.

The study points out that the collection and handling of personal data in this situation is not regulated in Australia. Even the use of a credit card does not bring it under the credit information rules of the Commonwealth Privacy Act 1988 because the credit-card issuer, not the retailer, would be the credit provider.

As for membership of industry associations, the report notes that “[b]efore long, members of both ADMA [Australian Direct Marketing Association] and the IIA [Internet Industry Association] are likely to be required to observe new codes of practice which should incorporate the Privacy Commissioner’s National Principles. ... 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 has anything approaching total coverage of businesses operating in the direct marketing or Internet industries respectively”.

It mentions the proposed Victorian legislation but concludes that “[i]ndividuals 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”.

Since the data might also pass through the hands of Australian carriers and service providers, the study examines their situation as well. It finds that a complex co-regulatory regime is being introduced in the telecommunications sector. Carriers and service providers are not only subject to the strict use and disclosure provisions of the Telecommunications Act 1997 to varying degrees but also to a number of codes of practice being developed by the Australian Communications Industry Forum. It is still unclear how content service providers (like the retailer in this case) will be affected by this co-regulatory regime.

**My scorecard: A clear failing grade in the case of content providers.**

**Sub-contracted data processing**

The final scenario contemplates a large Australian multinational corporation offering a complete range of data outsourcing services, such as traditional bureau processing, data warehousing, applications maintenance and network management. The study envisages a major European water utility company contracting with the outsourcing company to process its customer database with daily batch transfers to and from the European countries. The contract stipulates that ownership and control of any data processed remains with the European utility and the outsourcing company may only collect, process, use and disclose data as expressly authorised or as necessary to perform contractual obligations.

Again it is noted that the Internet Industry Association, of which the outsourcing company is a member, proposes adopting a code of conduct implementing the National Principles. Until this happens, the report suggests that the contractual provisions offer the best scope for privacy protection, since the services offered by the company are not subject to any statutory control. The rather damning conclusion is that “... privacy protection in Australian laws remain a patchwork quilt, applying only to limited sectors or narrow classes of data”.

**My scorecard: Another failing grade.**

**The other countries**

New Zealand and Hong Kong both have private-sector data protection laws similar to the EU. Their regimes came out of the study looking good. The USA, Canada and Japan have patchwork provisions reminiscent of the Australian situation.