PL&B Annual International Conference 2001 Reports

by Stewart Dresner

WITH A RECORD NUMBER of participants from 15 countries, including DPAs from 10 jurisdictions and nearly 50 speakers, the July conference reflects recognition of growing importance of consumers' privacy, and a need for companies to engage with new and stricter laws.

How can companies make privacy a competitive advantage?

Stewart Dresner, Chief Executive, *Privacy Laws & Business*

We can regard privacy as a law based human right representing one end of a continuum. From the legal standpoint in Europe, privacy is not a right to be bartered away for air miles, or discounts, or priority access to a higher level of service.

The other end of the spectrum, from the free market standpoint, is that personal data is a commercial commodity to be bought and sold. This is sometimes the case in list development for direct marketing, and the collection of online data by way of cookies when consumers often have no idea that data about them is being collected, used for other purposes, rented and/or sold.

I consider that the best companies can indeed make privacy a competitive advantage. Companies can use the vigour of the free market, with good design and organisational skills to strengthen the force of what can easily be seen as merely an abstract legal concept. These companies want to win and retain the trust of their customers and prospects.

The best companies take energetic steps to integrate privacy concepts into their operations, for example, by stating publicly their commitment to data security; respecting the wishes of those who do not wish to be mailed, faxed or e-mailed; prominently displaying a privacy policy on a website and keeping to their promises; and maintaining a vigorous and comprehensive management and staff training programme.

If you want to make privacy a competitive advantage, how would you do it?

1. Analyse what your consumers want in terms of privacy and whether you can integrate their wishes into your various business operations.

2. Develop a clear understanding of the various ways you could incorporate privacy values into your business which could enhance or reduce your competitive position.

3. Discuss the options with the appropriate managers and ask them to think outside the conventions of their discipline, for example, changing an opt-out to an opt-in, or giving two or three opt-out options rather than just one. Customers could then state, for example, that they want mail but not e-mail; they want to hear from you but not third parties.

4. Does your chief executive think that privacy is potentially a competitive advantage for your business? Can you put forward persuasive arguments that make sense in your business? If so, you stand a reasonable chance of obtaining the resources to put privacy programmes in place. If not, you are forced to work on defensive lines, such as "we have to do this job properly to avoid complaints and prosecutions."

5. Construct a plan of actions which are achievable within a few months, or even quicker – otherwise there is a risk that the programme will lose direction.

Once you make privacy a competitive advantage for your organisation, critics and advocates will always press you to go further. At first, that might sound troubling. But if you think of the analogy of car safety, competition to improve standards has led to improvements for everyone. Surely, in the long term, it would be more beneficial to your organisation for you to think of ways of enhancing the privacy values in *your* services.

This report is an edited version of Stewart Dresner's opening remarks at PL&B's 14th Annual International Conference, Cambridge, July 2nd-4th, 2001. This report, those following and many others are available on a CD-Rom from Privacy Laws & Business.

The New Dutch Data Protection Act

Diana Alonso Blas, LLM
Senior International Officer,
Dutch Data Protection Authority

Report by Eugene Oscapella

The new Data Protection Act was enacted on July 6, 2000 and will take effect on September 1, 2001. An English version of the Act is available on the Dutch Data Protection Authority's web site. The Act is implementing the principles of the EU Directive into the Dutch system.

One of the many differences between the old and new laws is the scope of application. The application of the new law is broader. The new law moves from a concept of registration of persons to registration of "processing." It covers processing from the moment of collection to the destruction of the information. Transparency is now the cornerstone of the system. The new law also gives individuals the right to oppose, and introduces clear regulation of transfers to countries outside the EU. As well, the Data Protection Authority is given the new powers.

The new law covers the activities of controllers with an establishment in The Netherlands. It also covers controllers not established in the EU but who use means situated in The Netherlands. This is much more controversial and difficult to define.

Transfers outside the EEA

The new law also provides very clear regulation of transfers to third countries outside the European Economic Area. The process of examining transfers must answer three questions:

1. Is there adequate protection in the receiving country? In the first instance, the data controller will make this decision, taking into account several elements, including decisions on adequacy made in Brussels. (see p.14)

2. If the controller concludes that protection is in the receiving country is not inadequate, does one of the exceptions (similar to those in Article 26 of the EU Directive) apply?

3. If there is no right to transfer under the first two categories, can the data controller use a contract? To do so, the controller must first obtain a permit from the Minister of Justice. The Data Protection Authority will help the Minister of Justice develop appropriate guidelines for such cases. These guidelines will be published on the DPA's web site. Under the new law, even if a data controller uses the European Commission's model contracts, the data controller must still apply to the Minister of Justice for a permit. However, if data controllers use the model contract, they will normally receive a permit very quickly.

Even if a country does not now have a declaration of adequacy from Brussels, this does not mean that the country fails the adequacy test.

New enforcement powers

The new law also gives the Data Protection Authority new enforcement powers. Before, the only weapon when someone did something wrong was publicity. The new law provides additional means for dealing with violations. In certain cases, the Data Protection Authority will be able to impose certain administrative measures to constrain violations any of the principles of the law. For example, people who fail to notify about their processing operations may be subject to an administrative fine of up to £3,000.

These powers are in addition to the penal provisions in the old law that have been transferred into the new law. In practice, these penal provisions are rarely used. The procedure for using them is quite complex, so the Data Protection Authority is pleased that there are now simpler means of enforcement available.

Four Track Policy

Enforcement is only one element of a four-track policy. One track involves increasing the awareness of citizens about data protection. The second track is legislation and self-regulation. The third track is technology, and the fourth is enforcement.

There was concern about the Data Protection Authority both advising government and having powers of enforcement, so care had to be taken to avoid a conflict.

If data controllers were in compliance with the current law, they will not need to worry too much about the new law. However, all data controllers will have to notify the Data Protection Authority again, even if they have notified it in the past. They will have a year to make this notification and to adapt to the new law.

The existing law contains many exemptions from the notification requirements. The new law contains even more exemptions.

(See also "Commission recommends easier access to personal data for Dutch law enforcement", at page 22)

New Data Protection Law in Germany

Dr Ulrich Wuermeling,
lawyer & partner, Wessing
& Berenberg-Gossler

Report by María Verónica Pérez Asinari

After the passing of the European Union Data Protection Directive 95/46/EC, some changes to Germany's legislative structure were necessary to transpose the Directive into a new law.

Germany's new law has been fully in force since May 23rd 2001. How has Germany interpreted the EU directive differently from other EU Member States and what are the practical implications for the private sector?

1) Article 5 of the EU DP Directive
This article provides that "Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful".

The German interpretation of this article is that the Directive provides a minimum standard, that there are no restrictions against stricter rules. This is not the case. There is a sort of flexibility within the provisions. That is the sprit of Article 5, in a way that it is possible to use different rules. But this does not mean that is a minimum standard, it is also a maximum standard in some provisions.

So, the effect of avoiding restrictions on the data flows within the European internal market is not fulfilled. Due to stricter rules in Germany there are still some problems that affect the common market.

2) New principle: Reduce data processing
The German Act introduced a new principle, the duty to avoid and reduce data processing.

It is described in Section 3a BDSG: "Design and choice of data processing systems shall take the aim into account to collect, process or use none or as little as possible personal data. In particular, the possibility to anonymise and pseudomise shall be used as far as it is possible and the effort is reasonable with regard to the envisaged purpose of protection."

Dr Wuermeling stated it is very difficult to know what precisely has to be done.

3) Chip cards
The new legal framework provides extended company duties to inform the data subjects about the functioning of the chip cards, how to enforce the right of access and the right to delete, and the measures to be taken in case of loss or destruction.

There is also a duty to provide technical service to access data stored in a device, and a duty to make communications with a device transparent for the data subject.

4) Video surveillance
The surveillance of rooms accessible to the public, with optical-electronic devices, is subject to extended duties to inform the data subject. Secondary use is permitted if it is necessary for public security or for detection of criminal offences. There is also a strict duty to delete the data recorded.

5) Direct marketing
Concerning direct marketing, processors have to comply with the obligation to inform the data subject, on request, about the right to object and about the source of the data. There are specific rules for certain areas like the Internet, telecommunications and postal services, where consent is needed before using the data.

6) Internal Data Protection Officer
This concept that also existed in the old law. Every company that has more than five persons working electronically should have an internal data protection officer. The amendments introduce new duties:

1. facilitating public access to the internal data processing register; this is due to the absence of a central public register for the private sector with all the registrations.

2. The internal data protection officer is also in charge of the prior checking procedure that was in the Directive.

7) Data Protection Authorities.
Under the old law, Data Protection Authorities had strong rights with regard to organisational and technical measures. Nevertheless, the rights conveyed concerning the lawfulness of data processing were ineffective. As a consequence of article 28 of the Directive, additional sanctions have been incorporated, as well as the right to bring violations to the attention of a public prosecutor.

Dr Wuermeling commented that some of these very rigorous regulations, a number of which are not imposed anywhere else in the European Union, do not favour the internal market. It is not possible to say that the goal of harmonisation has really been reached.

Dr. Ulrich Wuermeling is a lawyer and partner of the firm Wessing & Berenberg-Gossler, Frankfurt, and Co-editor of Datenschutz-Berater.
Tel: +49 69 971 300
E-Mail: u.wuermeling@wessing.de

María Verónica Pérez Asinari is a researcher at the Centre de Recherches Informatique et Droit, University of Namur, Belgium.

New Irish Law Imminent

Joe Meade, Data Protection Commissioner, Ireland

Case law has established that privacy as one of the unenumerated rights in Ireland's Constitution of 1937, although the Constitution itself contains no specific privacy provision. As recently as 1998, the Law Reform Commission said that privacy is more than instrumental to the achievement of other goals. It is a basic human right that applies to all persons.

The Data Protection Act of 1988 implemented the European Convention on Data Protection. It created rights for individuals and responsibilities for computer users. There is a balance between these rights and responsibilities.

The EU Directive will be transposed

The road to Germany's new data protection law

The first Data Protection Act for the public sector was passed in Hesse, in 1970. The German Federal Data Protection Act covering the private and federal public sector was enacted in 1977. There was a general review of this Act in 1990. This legal framework must be read in conjunction with chapter 11 of the Telecommunications Act, 1996; the Teleservices Data Protection Act, 1997; and additional sector specific regulations.

into Irish law by an amendment to the Data Protection Act of 1988. Because existing provisions of the Irish Act already closely reflect those of the EU Directive, the amendments will not be major. The wording of any amendments will very closely reflect the articles of the EU Directive.

The major changes concern manual data, data quality, the lawfulness of processing, informing the data subject, right of access, the right to object, automated decisions, notification and transfers to third countries.

How the EU Determines Adequacy

Fabrizia Benini, Data Protection Unit, Internal Market Directorate, European Commission, Brussels.

Report by Vivian Bowern

1. Principles and Declarations

The European Commission has been given a "tool" by the Directive in Article 25.6 to declare a third country's legislative or self regulatory arrangements sufficient to provide adequate protection to data subjects who have some of their personal data transferred to that country. This is a less demanding declaration than one of "equivalence".

The Commission has a power also to make a negative declaration. Such a declaration would only be made on a case by case basis affecting a particular transfer or class of transfer.

The principles on which an adequacy assessment might be made were set out by the Art. 29 Working Party of DPA representatives in July 1999.

A Commission assessment is binding on member states. They may not prevent transfers countries whose legislation or arrangements the Commission declares "adequate."

So far only Switzerland and Hungary have been granted "adequate" status on the grounds of their own national data protection legislation. Canada, in September, and New Zealand are expected to follow. The voluntary self-regulatory scheme in the USA known as "Safe Harbor" has also been granted "adequate" status. These "miracles do not happen very often but the process for granting an adequacy declaration is elaborate."

2. The Declaration Process

The process for assessing adequacy has four stages.

The Article 29 Working Party must first give an 'opinion' to the EU Commission. Only if this is favourable will the Commission proceed. In the case of the US Department of Commerce Safe Harbor scheme, critical observations led to over two years of negotiations and amendments before an adequacy declaration was made.

Once a favourable 'opinion' has been received from the Art. 29 Working Party, the Commission formally decides to proceed and seeks an 'opinion' from the Art. 31 Working Party of governmental representatives. A qualified majority is sufficient to allow a declaration of adequacy to be promulgated. However, for the "Safe Harbor" proposals, a unanimous opinion was sought and eventually obtained.

The fourth and final stage is scrutiny by the European Parliament. It cannot formally disagree with policy but can, within 30 days of its promulgation, challenge a decision on the grounds that powers have been exceeded. Parliament did in fact challenge the policy content of the "Safe Harbor" arrangement with the USA, only to be ignored! Parliament did, however, receive an undertaking of early review and report.

The Commission is in contact with a significant number of governments as they develop legislation. It does not wait until legislation is enacted before establishing contact with a view to making an adequacy finding.

3. Contracts between the parties

Adequacy can be established by contractual arrangement. With the exception of the UK such adequacy creating contracts must be approved by the appropriate national Data Protection Authorities. Notification of such approvals is likely to be shared among authorities on a restricted website. In the UK, the Information Commissioner has decided that it is up to exporting data controllers to assess adequacy and to act accordingly.

To simplify the contract process, on June 18th 2001 the EU Commission promulgated its own set of model contractual clauses for transfers between data controllers which need no further approval from national Data Protection Authorities. These are available on the Commission's web-site. It has also invited other bodies such as the ICC and the UK's CBI to submit alternative sets of contractual clauses which it might prepare approve with similar effect. These standard clauses are the first of a series. They are not compulsory. They are off-the-shelf instruments to be used where appropriate.

The transfer of data between data controllers in Europe and data processors in third countries is the subject of a different set of model contractual clauses involving the additional requirements of Article 17 of the Directive. The EU Commission is currently consulting with interested parties, including the CBI in the UK.

The US Safe Harbor: Why are more ships not docking ?

Robert Ellis Smith,
Publisher of Privacy Journal, USA
www.privacyjournal.net

Report by Vivian Bowern

By September 17th 2001, 102 organisations had entered the Safe Harbor. However, by late June, only 67 companies had signed up. The biggest multinational name was Hewlett Packard in respect of customer data. The 67 were mostly dot com companies. The information intensive companies had in general not signed up. Separate regulation affected insurance, credit referencing and financial services generally and these sectors would not be expected to sign up.

Why so slow?

There were five reasons why companies had not signed up:

First, there was no public pressure

to do so. Safe Harbor gave rights to European citizens but not to American citizens. The speaker's sister in Holland could see and require amendments to her American Express record: he could not.

Second, there was no governmental pressure until recently to conform to data protection principles.

Third, there was no corporate pressure. Indeed, the reverse was true. To sign up to the principles was to make a permanent and generalised commitment for data collected under them. There was a view that an information-intensive company would have its value reduced by doing so.

Fourth, there are alternatives, for instance, consent given in Europe, not processing European data outside Europe, and the use of specific contracts.

Fifth, there was also a wait-and-see culture to see what proceedings would arise and then to judge the issue.

For further Safe Harbor information visit www.export.gov/safeharbor

The Hewlett Packard Privacy Program

Barbara Lawler, Customer Privacy Manager, Hewlett Packard, USA

Report by Vivian Bowern

Hewlett Packard's guiding principle to its relationships with its customers is that it allows them to control their own data. They are given choices to enhance trust. "Customers information belongs to them:" Carly Fiorina, CEO of HP.

It was the view of the Arthur Andersen organisation in 2000 that "Privacy has become the most significant obstacle to the continued success of e-Business ventures." HP believes that customer trust is vital to overcoming this obstacle.

The privacy policy is universally applied in all countries in which HP does business. It has five fundamentals.

1. The Five HP Privacy Policy Fundamentals

1. *Awareness:* There is a notice of policy on every hp.com home page.

2. *Choice:* HP does not sell customer data. Third party data sharing is opt-in only. Customers can opt out of personal data collection and contact. HP will move to opt-in for e-mail by late 2001.

3. *Access:* Customers may view, correct and amend, but not necessarily online.

4. *Security:* Sensitive and most personal data transactions are encrypted.

5. *Oversight:* HP commits to strong privacy principles and practices through the BBB Online Privacy Seal Program and Safe Harbor Certification. There is an internal path for customers to escalate issues. External audit and dispute resolution for customer disputes is provided for.

Each of these five fundamentals has its own set of rules.

2. Why Safe Harbor for HP?

It provides consistency and manageability for HP intra- and inter-country business operations. Practices required were already in place through BBB Online Privacy Seal Program. HP did not want to be in the contracts business.

Hewlett Packard was a founding member of Safe Harbor in respect of its customers. It plans to affiliate in July 2001 in respect of its employees.

3. Partner Management

HP includes privacy policy requirements in contracts with partner companies where customer data is shared. Partners are required to comply with all privacy laws and to publish a privacy statement. Partners may not share HP customer data unless customer has consented. Partners may not collect personally identifiable data on HP.com pages.

Privacy Protection for Online and Offline Marketing in the USA

Robert Belair, Attorney & Partner, Mullenholtz, Brimsek & Belair, Washington DC and Editor, *Privacy & American Business*, USA.

Report by Peter Carey

The United States is in the midst of a privacy revolution. Currently the use of personal data for marketing purposes is largely unregulated. This is set to substantially change in the next few years, but it is not yet clear whether the US will go down the 'notice and opt-out' route or the 'opt-in' route.

There is a substantial quantity of privacy legislation in the US, but it is largely sector-specific. One example is the Children Online Privacy Protection Act (COPPA), which requires verifiable parental consent in order to collect data on children under the age of thirteen.

Another example is Health Insurance Portability and Accountability Act, which regulates the use and collection of health-related information and requires privacy training and the appointment of a Chief Privacy Officer. Over seven thousand privacy bills are introduced in the State legislatures every year (5% of all state legislative business) in particular sectors such as credit reporting, financial instruments and insurance. Several notorious Internet privacy-related lawsuits have been heard in the last few months. Examples are those involving Doubleclick, AOL and ToysR'Us. In Michigan v AmericanBabies.com, the first cookies case brought by a state Attorney-General, the State of Michigan is seeking to curtail the use of information on users who visit certain sites providing baby products and information.

As far as marketing is concerned, the US has no current regulation. There are three reasons for this:

1. Marketing data are not used to make substantive decisions concerning individuals (use);

2. The information is usually derived directly from the consumer himself (source); and

3. It is accessed by personal characteristics or geographical location ('zip-plus-four') rather than by name (content).

continued on page 23