

## PRIVACY ON THE NET

### Introduction

The business advantage of the Internet is its ability to provide large quantities of data to any number of locations virtually anywhere in the world. However, this often involves handling personal information about individuals, be they employees, customers or target clients. Any business must be aware of its legal obligations to individuals regarding the use of personal data.

### Confidentiality

Traditionally English law did not recognise a right to privacy. However the law of confidence goes some way to providing protection for information held on individuals and commercially sensitive information in the absence of an express right to privacy.

The case of *Coco v AN Clerk (Engineers) Limited* 1969 laid down three necessary elements for a breach of confidence:

- 1) The information must have the necessary quality of confidence about it.
- 2) The information must have been imparted in circumstances importing an obligation of confidence.
- 3) There must have been unauthorised use of that information to the detriment of the party communicating it.

Each of the three requirements has been the subject of case law. However, the common theme is that confidential information is capable of protection.

### Data Protection

This can be contrasted with the data protection legislation in the UK which is based on an individual's right not to have personal data held relating to him or her disclosed to third parties. These rights were first introduced by the Data Protection Act 1984 which protected an individual's rights of non-disclosure of personal data held on a computer and have been broadened by the Data Protection Act 1998 ('DPA') (see the Guideline on the Data Protection Act 1998). The DPA itself implements the Data Protection Directive (95/46/EC of 24 October 1995).

The thrust of the legislation is that individuals must be informed about information obtained concerning them and in many circumstances their consent must be obtained before any information is used. In addition, the DPA contains data management requirements.

The DPA will directly affect e-business and how it handles and processes information about individuals.

The DPA broadly states that

- (a) the data controller must obtain the consent from the data subject before processing personally identifiable data about the data subject, (with a limited number of exceptions);
- (b) the data controller must notify its activities to the Information Commissioner;
- (c) the data controller must comply with the eight data protection principles; and
- (d) an individual can request to see personal data regarding him or her and object to certain processing such as processing of data for direct marketing purposes, and claim compensation in certain cases.

The overriding principle is that data must be processed fairly and lawfully. The data controller must inform individuals about any processing of data. The processing must be for a specified purpose which concerns individuals. In addition, one of the following must be met, either: (a) the data subject must give his or her consent to the processing of data for a specified purpose; (b) the processing must be necessary in relation to a contract to which the data subject is a party; or (c) the processing of data must be in the legitimate interests of the data controller except where and warranted by reason of prejudice to the rights and freedom or legitimate interest of the data subject. Data must be kept up to date and its use must not be excessive for the specified purpose. The data must also be kept secure and held for no longer than is necessary. Data cannot be transferred to countries outside the EEA to countries that are deemed not to have adequate protection for personal data (see the Guideline on Data Protection (Transfer of Data Outside EU)).

### **Trading in Data**

The disposal and acquisition of customer lists and data will inevitably grow in importance as insolvent dotcoms seek to sell this information as part of their assets. So far, the nearest situation was a sale by liquidators of Boo.com of its customer lists to a New York company and this sale was the subject of some debate concerning the ambit of its privacy policies. Companies based in the EEA should therefore only treat their customer lists as an asset where they have clearly stated on the website or in documents received by their customers that those lists may be transferred to third parties for use by those third parties. Consent should also be obtained not only to transfer to third parties but also to the transfer of the data to outside the EEA to allow an easy sell to non-EEA based purchasers.

### **Cookies**

Cookies enable website operators to build up a profile of its users including their IP address and surfing history. Such information might be considered anonymous since it does not usually identify individuals. Use of cookies under the DPA has been unclear and it has been the common view that retrieval of data through a cookie that is not linked to other personal information e.g. user's name or e-mail address, will not fall within the scope of the DPA, because of the anonymous nature of the data.

However the Information Commissioner has indicated that in her view the use of cookies may fall within the scope of the DPA.

The fact that cookies may fall within the scope of the DPA does not mean that it is prohibited. Website operators can still continue to retrieve data through the use of cookies quite lawfully provided the appropriate steps are taken. Such steps include:

- Displaying a Privacy Policy on their website identifying themselves and a point of contact for the user.
- Informing users about all uses (including the use of cookies if used) and disclosures of their information.
- Obtaining consent from the user to process the data collected, through the use of either an opt-in or opt-out box.

On 7 December 2001, the Council of Telecommunications Ministers amended the recommendations of the European Parliament on the proposed directive concerning the processing of personal data and the protection of privacy in the electronic communications sector (known as the Telecommunications Data Protection Directive), to permit the use of cookies without the need for prior user consent, provided the website operator gives clear and

precise prior information on their use to the user. The website operator should also give users the opportunity to refuse to have a cookie stored on their computer.

### **Privacy Policies**

In the UK a privacy policy incorporated onto a website serves two functions. The first is to facilitate the e-business in fulfilling its legal obligations under the DPA. This can be contrasted with the situation in the United States where historically there have been no data protection laws (although there are movements to change this). However the second and overriding objective is to install confidence in the user that information will not be disclosed to any third parties, and this objective is common to both jurisdictions.

Many businesses both in the EU and elsewhere have introduced privacy policies which aim to give the customers of and visitors to a website a degree of control, confidence and protection in respect of personal or commercially sensitive information. The increased use of privacy policies on websites further demonstrates the importance attached to privacy in maintaining public confidence in e-business.

In 1998, 71% of the top 100 websites had privacy policies and that percentage has now increased to 94%. In September 2000 Amazon.com was publicly criticised for changing the terms of its privacy policy allowing the transfer of customer data to third parties without seeking additional consent from its customers. Amazon.com stated that its customers' data formed part of its assets and might be traded, and this remains Amazon.com's stated position. In the recent Toysmart.com case, Toysmart.com found its attempts to sell its customers' information contrary to its privacy policy on its website (which stated it would never share the information with any third party) subject to legal action by both the US Federal Trade Commission and the Attorney Generals of 44 US States for breach of promise and misrepresentation. The FTC indicated that Toysmart.com had sought to transfer the data together with the goodwill in its business to a third party. It was held that data will not be regarded as being used fairly or lawfully unless the data subject has consented to that use.

Since the incorporation of the European Convention on Human Rights ("Convention") into UK law through the Human Rights Act 1998 ("Act") in October 2000, e-businesses must also give consideration to Article 8 of the Convention, which enshrines an individual's right to respect his private and family life, his home and his correspondence. Although the rights under the Act are only enforceable against public authorities, it is a requirement of the Act that domestic legislation will be interpreted so as to be compatible with the Convention rights and it is therefore essential when considering compliance with the law, including the DPA, to consider Article 8 and other Convention rights.

There are a number of provisions that a privacy policy should contain:

- The identity of the controller of the data, and a clear indication as to how the data will be used.
- Details of those to whom the information will be transmitted and whether the information is likely to leave the EEA.
- All means of gathering information should be made clear, including cookies.
- Sensitive data must be collected only if explicit consent as to its use has been obtained from the data subject.
- A statement making clear that subjects have a right to see information held.
- An opt-out box providing an opportunity to decline consent for the collection of information.
- Details of safeguards for information transmitted outside of the EEA.

## **Executive Summary**

- The DPA and the law of confidence protect information relating to an individual.
- Data controllers must obtain the consent of an individual before they process information relating to an individual (subject to a limited number of exceptions). Explicit consent must be given for sensitive data.
- A data controller can process data relating to an individual without his or her consent if it is in the legitimate interests of the data controller to do so, but the amount of this is not clear.
- Privacy policies should be incorporated onto websites. They enable site operators to comply with its obligations under the DPA.
- Privacy policies also give the site user confidence.

**© Davenport Lyons 2001. All rights reserved**

**This document reflects the law and practice as at May 2002. It is general in nature, and does not purport in any way to be comprehensive or a substitute for specialist legal advice in individual circumstances.**