Blake Lapthorn Linnell

PRIVACY AND DATA PROTECTION IN THE UK IN 2006 (A brief overview):

Data Protection Act 1998

- Legislation primarily applies to data controllers (persons legal and natural who dictate the purposes for which and the manner in which personal data is processed).
- Annual obligation on data controllers to notify processing to the Information Commissioner. One notification per company in a group. There are bogus agencies that send threatening letters that appear official, to companies that are not notified, and ask for up to £80 to make the notification – when in fact it costs only £35 annually when done directly with the Information Commissioner.
- Data processors are persons legal and natural who process personal data on behalf of data controllers. Data processors need not notify the processing they undertake on behalf of others.
- Personal data is processed in accordance with 8 data protection principles.
- Definition of personal data is based both on type of data and manner of processing. If data is personally identifiable information but processed in a manner not caught by the definition, then it will not be personal data.
- Categories are:
    - Automatically processed,
    - Information recorded with the intention that it will be automatically processed,
    - Relevant filing system (highly structured manual system),
    - Accessible record (a manual housing, social services, medical or LEA education record),
    - New category since 1st Jan 2005: unstructured personal data – any personal data that is processed by a public authority that does not fall into any of the other categories. Introduced by the Freedom of Information Act.

- **Durant v Financial Services Authority (2003)** – had the effect of narrowing the definition of personal data from the statutory definition (in addition to being information from which a living individual can be recognised, information now needs to be focussed on the individual and significantly biographical and capable of adversely affecting privacy too). In practice this means that there are some strange results in terms of what is and is not protected. Some would say an element of common sense now prevails, but the European Commission has said that it does not consider that this case is in line with the Directive behind the DPA 1998.

- **Durant V Financial Services Authority** has also changed the definition of a relevant filing system. To be a relevant filing system the set of data has to be so highly structured, that at the outset of a search for a particular piece of personal data, the location of that personal data can be determined with as much certainty as one might obtain from a computerised search. The courts also cited “the temp test”. Would a temp be able to locate the information from the filing system alone, with minimal reference to knowledgeable permanent staff?

Freedom of Information Act

- Relevant for foreign organisations doing business with English public authorities. Anyone, anywhere, without proof of identity has the right to access recorded information held by a public authority. Public authorities have no right to question motive.
- Could lead to release of information about a company, or information supplied by it.

- There are exemptions for information supplied in confidence (s41) and information the disclosure of which would prejudice commercial interests (s43(2)), but the latter is subject to the public interest test. That means that if the public interest in withholding the information does not outweigh the public interest in disclosing, then the information must still be disclosed, notwithstanding that it is damaging.
- Information Commissioner and Office of Government Commerce have taken a surprisingly liberal view on this, and generally uphold the fact that there is a public interest in ensuring that private sector bodies are not dissuaded from doing business with the public sector for fear of damaging disclosures.

Confidentiality

- No criminal penalties as in other jurisdictions as the Common Law does not recognise property in information.
- Protected by a common law right to confidentiality (breach = civil wrong or tort), or contract (breach = breach of contract).
- Freedom of Information Act (s41) only protects information that falls within common law definition of confidential information which has caused problems with contracts signed before 1st Jan 2005, which seek to protect wider classes of information from disclosure.

Regulation of Investigatory Powers Act 2000

- Governs interception of communications on private communications systems, such as e-mail and telephone and creates the tort of unlawful interception. Of particular import to companies wishing to monitor their e-mail. When RIPA came in, there were fears that monitoring would have to stop over night. However, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 were then made under RIPA that allow monitoring in limited circumstances where reasonable steps are taken to alert all users of the monitored system (including external) of the fact that monitoring is taking place. From a **DPA** perspective, businesses monitoring communications need to inform users that the monitoring is taking place in order to fulfil fair processing requirements. From a **Human Rights Act 1998** perspective, the benefits to the organisation of the monitoring have to be proportionate to the infringement of the qualified right to privacy of correspondence, where personal e-mails are likely to be accessed. In practice policies should tell users to mark personal e-mails "personal" so that appropriate safeguards can be put in place.
- English regulations are relatively easygoing, and many multinational companies that are based in England find it hard to come up with a universal e-mail monitoring policy that is lawful in every country. (In the US it varies from state to state, and in some European countries it is totally unlawful).

- **Privacy and Electronic Communications (EC Directive) Regulations 2003** now govern marketing by electronic means. (email, telephone, fax, sms etc). This originates from a directive, so similar provisions should be in place around Europe – however ours are typically pragmatic – there are no restrictions on marketing to business e-mail addresses. For private e-mail addresses consent is required, but this can be obtained from a "soft opt-in". The soft opt-in occurs where the individual has given their details as part of a request for information about products, or negotiations for a sale or a sale, the marketing is for similar goods and services, and the individual has had the opportunity to opt out of receiving marketing e-mail.
- Breach of the Regulations (including breaches incurred by making direct marketing calls using fax or telephone to those persons who have registered with the Fax Preference Service and the Telephone Preference Service) can lead to enforcement action by the Information Commissioner who can issue an enforcement notice. It is a criminal offence to fail to comply with an enforcement notice, and there is personal liability for directors, managers, secretaries and other officers where the corporate body commits the breach and the failure occurs with their consent or connivance, or due to their neglect. Corporate subscribers now have the right to register with the Telephone Preference Service.

English Pragmatism

- When the DPA was implemented, there were fears that principle 8 (personal data shall not be transferred to other countries unless there is adequate protection for the rights and freedoms of data subjects) would inhibit trade. Of particular concern in England was the fact that the US was deemed not to have adequate laws. In practice fears have proved unfounded:
    - It has always been open to data controllers to assess "adequacy" themselves;
    - Consent will validate the transfer (if data subjects are informed as to the country involved);
    - EEA countries are deemed adequate, and there is a permitted list of countries approved by the EU Commission. The expansion of the EU has helped;
    - Safe Harbour provisions have been adopted by large US companies;
    - There are EU authorised data transfer clauses;
    - There are a great deal of exceptions to principle 8 in Schedule 4, and
    - A good old data processor agreement is likely to ensure adequate protection.
- Confusion however, still abounds, and this is exploited by groups that are opposed to outsourcing services to India, such as the unions. In reality principle 8 is an obstacle that can be easily overcome.
- Durant v FSA has provided some pragmatism re relevant filing systems and definition of personal data.
- There was a rash of high profile cases recently that lead to criticism of the DPA as being too complicated and restrictive (when in fact in both cases the wrong arose from misinterpretations of the law): e.g. Soham, the fact that Ian Huntley's details had been partially deleted by the police and that vital details weren't passed between police forces. See: http://news.bbc.co.uk/1/hi/uk/3395071.stm E.g. Old couple dying because British Gas failed to pass on to social services the fact that their gas had been cut off. http://www.out-law.com/page-4197 http://news.bbc.co.uk/1/hi/england/london/3342059.stm
  The latest Information Commissioner Richard Thomas immediately issued a statement that organisations cannot use the DPA to justify unacceptable practices, and has called for a simplification of guidance on data protection. Guidance notes are now significantly more practical and specific than previously (see www.dataprotection.gov.uk)
- The Department for Constitutional Affairs has a project which is looking into how the current Act might be simplified to make it easier to understand.
- The EU Commission has a working party to simplify fair processing information to come up with "standard" data protection notices.

Privacy/Image rights etc

- The common law always regarded "the light reflected from a person" (their image) as being in common ownership.
- Famous people could prevent reproduction of their image for commercial purposes as it infringed their economic right to profit from such reproduction. The ordinary man had no such right.
- Various attempts have been made to use The Human Rights Act right to privacy to extend these rights to ordinary Joe. These have met with limited success as they run into the problem of famous people and press freedom.
- The Advertising Standards Authority and the other bodies that regulate advertising in the UK have stepped in by making it contrary to their codes of conduct to use images of recognisable people (famous or not) in advertising without their consent. Pixellated man has arrived!
- Whilst this only applies to regulated advertising (so excludes self produced brochures, website ads etc) there is an increase in ground level opinion that the individual does have the right to prevent (and thus charge for) use of their image for commercial purposes.

Geoffrey Sturgess
Blake Lapthorn Linnell
Geoffrey.Sturgess@bllaw.co.uk