Protecting Confidential Database Information

Martin Howe QC
8, New Square
Lincoln's Inn
www.8newsquare.co.uk

Reasons for protecting confidential information

- Value of information to one's own business - value to competitors
- Legal duties owed to customers and others to protect their confidentiality
- Reputational damage if confidential information is misused or leaked

Legal steps to ensure protection

Ownership of IP rights and duties of confidence

- Employees: ownership of IP rights generally OK but explicit clauses do no harm; helpful explicitly to impose duties of confidence re employer's and customers' information
- Contractors: (including one-man full time in-house): explicit ownership clauses essential; should also explicitly impose duty of confidence
- Right to take work product and use others to modify/update it

What can be protected by confidence

Proprietary methods as well as specific data

- Software: valuable in itself but may also incorporate confidential business methodology, e.g. trading algorithms
- Public website cannot be confidential BUT a transactional engine behind it may be; or a website behind password protection may be if terms and conditions of access so provide
- Database structure
- Own business and financial data
- Customers' and other third parties' confidential data
- Generally not protectable: skills and general techniques which form part of employees' own stock of skills and knowledge, even if acquired or developed working for a particular employer

Obligations regarding personal data

Data Protection Act 1998 (UK); EC Data Protection Directive

- Personal data defined as “data which relate to a living individual who can be identified” - s.1(1) DPA 1998.
- “Focus” test of English Court of Appeal in *Durant v FSA*, but will this be upheld by European Court?
- 7th principle: “Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.”
- 8th principle: no transfer of data outside the EEA except under “safe harbour” principles
- Other requirements (consent, fairness, use for other purposes, notices, access rights, accuracy, keeping up-to-date, retention when no longer required) outside scope of this talk

Litigation and its causes

Litigation often results from deficiencies in contractual or practical arrangements

- Defective or unclear contractual arrangements - lack of clarity as to ownership of IP rights or obligations of confidence
- Poor controls and policies over handling of confidential data: company laptops; data at employees' homes or on home computers; private use of company email systems; USB sticks
- Plain dishonesty: disgruntled ex-employees/contractors

Litigation against the dishonest

A combination of investigatory, technical and legal measures

- Investigation phase - expert assistance often needed for technical investigation, under cover work (e.g. trap orders) or surveillance
- Search orders (known as *Anton Piller* orders); asset freezing orders; disclosure orders; injunctions
- Computer forensics - hard disk imaging and court control of disclosure process

Special kinds of interim orders

Pirates and fly-by-night operators

- Search (*Anton Piller*) orders: intrusive, expensive but effective and sometimes essential
- “Doorstep Pillers” (immediate disclosure of e.g. computer software)
- Freezing orders
- Orders against ISPs (note special protection from liability under E-commerce Directive)
- Special forms of service e.g. by email