



FARRER & Co

Official Legal Partner

Farrer & Co/LMN Seminar

Legal Issues Associated with IT Service Provision: 25 April 2005

Anthony Misquitta - (Solicitor, Farrer & Co)

Background Legal Issues - (the Law outside of the Contract)

Protection for Software: The Basic Premise

The basic premise in the UK is that software is protected under the law of copyright as a “literary work”. Copyright protects the lines of code that make up the software in the same way that it protects the lines of text that make up a novel. Copyright is infringed if all, or a substantial part, of the work (the code) is copied.

Software, as such, can never be patented even if it amounts to a novel invention. The exception is where software forms part of an invention with other non-software elements.

This is in contrast to the position in the US where pure software patents can be obtained.

The Copyright Directive

This 2001 EU Directive was incorporated into UK law by the Copyright and Related Rights Regulations 2003 which came into force on 31 October 2003.

The main developments under the Directive and Regulations are:

1. it confirmed that “communication to the public” of a work infringes the copyright in it. Until then it was unclear if the posting of a work on a site infringed the copyright in it;
2. it confirmed that copying for the purpose of commercial research is not permitted; and
3. it criminalised the circumvention of copy-protection devices.

“The Software Patents Directive”

This Directive is actually called the “Directive on the Patentability of Computer-Implemented Inventions”.

Remember: patents involving software, provided the invention makes a technical contribution, have been granted for over 30 years.

Current EU law excludes certain types of inventions, in particular computer programs "as such". However, these exclusions have been interpreted differently across the EU.

The purpose of the Directive is twofold:

1. to harmonise the law in member states; and
2. to prevent a drift towards the more liberal approach taken by the United States.

The Directive makes it clear that a computer program on its own cannot be patented however it is expressed. Such programs will remain protected by copyright.

The Directive also ensures that the association of a computer with an invention will only be considered an invention if that combination makes a contribution beyond the normal running of a program, thus ensuring that general business software on its own cannot be patented.

A claim to a computer program, either on its own or on a carrier, shall not be allowed unless the program would, when loaded and executed in a programmable computer, programmable computer network or other programmable apparatus, put into force a patentable product or process claimed in the same patent application.

Navitaire v. EasyJet

Navitaire produced a software product called "*OpenRes*" which was a set of programs for airline booking systems

BulletProof Technologies produced a very similar set of programs for EasyJet which used the same ideas and technology but expressed them in different code.

Navitaire argued that:

“In the same way that copyright subsisting in a literary work may be infringed by a change in medium in which all that is taken is the plot, so also, it is said, may the copyright in computer software be infringed when the functional structure of the code is appropriated by writing different code which, put crudely, works in the same way.”

Navitaire 's contention was that BulletProof Technologies closely studied *OpenRes* and produced a system for EasyJet which operates in the same way from the user's point of view. They argued that copyright should protect "business logic" or "look and feel" of computer software programs even where the source code and architecture have not been copied.

The Court said whether or not BulletProof Technologies lifted Navataire's technology, this would only be a copyright infringement if it copied the lines of code, or substantial parts of them. BulletProof Technologies had not done this.

Databases

- "Databases" are collections of data or other material that are arranged in such a way so that the items are individually accessible by electronic or other means. They are protected by copyright but only if by reason of the selection or arrangement of the contents of the database the database constitutes "*the author's own intellectual creation*".
- "Database Right" protects databases where there has been a substantial investment in the obtaining, verifying or presenting of the contents of the database.
- Database right is infringed if all or a substantial part of the database is extracted or re-utilised (and repeated and systematic extraction of insubstantial parts can amount to a substantial extraction).
- Lasts for 15 years (but a new database right can be created in the same database whenever significant modifications occur).

British Horse Racing Board v. William Hill

The European Court have indicated that BHB do not have database rights in its database of horse racing data as it had not made a sufficient investment in obtaining the contents of the database. According to the ECJ, '*obtaining*' means '*seeking out existing independent materials*' and not '*the creation of materials*'.

BHB had spent considerable time and effort creating the data but the ECJ found that this was simply part of the process of putting together the pre-race information, including name, place and distance of races, and details of the horses. The ECJ said that the '*resources used to draw up a list of horses in a race ...do not represent investment in ... obtaining*'.

Liability for Content

The Electronic Commerce (EC Directive) Regulations 2002 provides certain defences for "Service Providers" whose networks or systems are used for unlawful purposes. The defences are broken down into three headings:

"*Mere Conduit*" where the Service Provider is merely transmitting content provided by a user, and this results in an infringement taking place. For example: where a user uses the University's system to

access infringing copies of a work, those copies are technically made by the University at the user's request. Article 12 of the Regulations would provide the University with a defence, provided that the University did not actively initiate the copy, send out copies or select/modify the copies.

"*Caching*"

where Internet messages are relayed from one computer to another through other computer servers. These passive intermediaries 'cache' the messages in question. Where those messages contain infringing material, the intermediaries are technically making infringing copies by caching the information. Provided the caching is passive, the intermediary will have a defence under Article 13 of the Regulations.

"*Hosting*"

where a Service Provider allows third party material to be hosted on their servers, the 'host' is also technically copying the material onto its server and indeed authorising others to copy it. Article 14 of the Regulations provides such a host with a defence where it has no actual knowledge of the infringing activity and it removes the infringing material as soon as it is made aware of it. In addition, by Article 15 of the Regulations, the Service Provider is not under any obligation to monitor the content on it.

The Defamation Act 1996

By section 1 of this Act 1 the person responsible for an intranet or website has a defence in respect of any claim that he/she is liable for defamatory comments made on that intranet or website if he/she can show that:

1. he/she was not the author, editor or publisher of the statement complained of;
2. he/she took reasonable care in relation to its publication; and
3. he/she did not know, and had no reason to believe, that what he/she did caused or contributed to the publication of a defamatory statement.

Therefore, if you host but do not edit the content, you will be entitled to the defence. But if you edit content and allow a defamatory comment to be made, you could be liable for it.

RIPA

The Regulation of Investigatory Powers Act 2000 (RIPA) must be read alongside the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (LBP Regulations).

RIPA states that the only means by which a company or institution can lawfully intercept its employees' or members' communications is with consent. The main purpose of the Act is to ensure that the relevant investigatory powers are used in accordance with human rights.

The LBP Regulations provide for circumstances where in a business context it is lawful to intercept communications (telephone and e-mail) without the employees'/members' consent. These are circumstances when the company/institution desires to:

- (a) establish the existence of facts relevant to the business;
- (b) check that the business/institution is complying with self-regulatory practices or procedures;
- (c) ensure that appropriate quality standards are maintained;
- (d) prevent or detect crime;
- (e) investigate or detect unauthorised use of the telecommunications system; and/or
- (f) ensure the effective operation of the telecommunications system.

However, recording should be limited to circumstances where it is *necessary and relevant* to the employer's/institution's business. Also, businesses/institutions should make *all reasonable efforts* to inform people that monitoring is taking place.

Tips:

1. Make it clear to users of your system that you are monitoring their use of the system (including their personal emails/calls) in order to ensure compliance with your use policies.
2. **ONLY** monitor in order to ensure compliance with your use policies.
3. Beware of monitoring staff use and using the results in the context of disciplinary proceedings or dismissals.

Spam

There are now two Regimes:

1. the regime under the Data Protection Act 1998; and

2. the regime under the Privacy and Electronic Communications (EC Directive) Regulations 2003.

Any email address that amounts to personal data must be “*processed*” in accordance with the Data Protection Principles and that normally involves seeking the consent of the data subject.

Under the Regulations, where the email address is that of “an individual subscriber” rather than “a business/corporate subscriber” further restrictions apply if you wish to send that individual “unsolicited commercial email” (which also included SMS messages). Put very simply you must either:

- (a) have obtained the individual subscriber’s prior consent to send them unsolicited commercial email; or
- (b) show that you have an “existing customer relationship” with the individual subscriber *and*:
 - (i) the marketing is in respect of the same kind of goods/services that you provided to them or discussed with them before; and
 - (ii) at the time that the individual subscriber gave you their email address they had an opportunity to refuse to allow you to use their details for marketing purposes (an opt-out).

In all unsolicited commercial emails to individuals, you must make it clear who is sending the email and you must give the recipient an easy way to indicate that they no longer wish to receive unsolicited commercial emails.