Critique of the Proposed UK Implementation of the EU Copyright Directive

Julian T. J. Midgley (jtjm@uk.eurorights.org)

August 21, 2002

Abstract

The UK Patent Office published its consultation paper on the implementation of the European Copyright Directive (2001/29/EC) on 7 August 2002, thus opening its consultation period on the directive. Responses to this paper must be submitted to the Patent Office by 31 October 2002. This paper is a critique of the proposed implementation; it highlights flaws in the proposal, and makes recommendations for their solution. It is intended to be useful both to those writing responses to the Patent Office, and to those who merely want to know how the implementation of the directive is likely to affect them.

1 Introduction

The proposed UK implementation (hereinafter referred to as the Proposal[1]) of the European Copyright Directive (2001/29/EC)[2] (the Directive) will bring about various changes in UK Copyright Law, the most significant of which concern the use of technological measures to protect copyrighted works, and the circumvention of those measures. This document analyses the Proposal, identifies flaws in the implementation and proposes solutions to them; in doing so it only considers solutions that are compliant with the Directive itself.

Although the Directive itself might be criticised in various ways, no attempt is made to make that criticism here, since the Directive has been passed, and the UK must implement legislation that is compliant with it as it stands.

2 Research into Cryptography

Paragraph (48) of the preamble to the Directive[3] requires that the legal protection against circumvention of technological measures not hinder research into cryptography. However, nothing in the Proposal affords cryptographers any protection against prosecution. In consequence, it is to be expected that the Proposal will result in chilling of cryptographic research, as has already been seen as a result of the Digital Millennium Copyright Act (DMCA) in the United States.

Academic cryptographers review algorithms proposed by their peers, examine algorithms and devices used by industry, and in the ordinary course of events, publish the results of their research, to assist in the advancement of knowledge of cryptography, and to enable flaws in algorithms to be corrected. Technical protection measures applied to copyrighted works frequently involve the use of cryptographic algorithms, and often make use of

[1]Proposal available from: http://www.patent.gov.uk/about/consultations/eccopyright/index.htm

[2]Directive available from: http://europa.eu.int/information_society/topics/multi/digital_rights/documents/index_en.htm

[3](48) Such legal protection should be provided in respect of technological measures that effectively restrict acts not authorised by the rightsholders of any copyright, rights related to copyright or the sui generis right in databases without, however, preventing the normal operation of electronic equipment and its technological development. Such legal protection implies no obligation to design devices, products, components or services to correspond to technological measures, so long as such device, product, component or service does not otherwise fall under the prohibition of Article 6. Such legal protection should respect proportionality and should not prohibit those devices or activities which have a commercially significant purpose or use other than to circumvent the technical protection. In particular, this protection should not hinder research into cryptography.

known algorithms that are used for a variety of purposes, many of which may have nothing whatever to do with technical protection measures. As it stands, the proposal hinders research into cryptography in the following ways:

1. In the process of investigating an algorithm, a cryptographer may discover weaknesses in it, and confirm those weaknesses by demonstrating that an attacker can obtain the plain text of an encrypted message. If the algorithm concerned formed part of a technical protection measure, this process would amount to circumvention of that measure, thus making the academic concerned civilly liable to prosecution under 296ZA of the Proposal.
2. In the usual course of events, academics publish the results of their research in academic journals, and often on their websites. In the case where their research concerned (incidentally or otherwise) the circumvention of a technical protection measure applied to computer programs, publication would make the researcher liable to prosecution under section 296 of the proposal. If the protection measure was applied to something other than computer software, the situation is less clear, but it seems probable that 'publication' would constitute 'provision of a service' for the purposes of 296ZB and 296ZC of the proposal, making the researcher liable to both criminal and civil prosecution.

There are no provisions in the Proposal that protect cryptographic researchers from prosecution. That there is a real danger of their being pursued by those companies whose protection measures they circumvent is evidenced by the case of Professor Felten in the United States, who was threatened with a civil suit under the DMCA when he announced his intention to publish research demonstrating weaknesses in a watermarking technology proposed by the SDMI Foundation[4].

The lack of protection for researchers would seem to make the Proposal non-compliant with the Directive. It is therefore important that some such provision is made available.

2.1 Recommended solutions

Language must be introduced into the Proposal providing cryptographic researchers with immunity from prosecution under the terms of sections 296, 296ZA, 296ZB and 296ZC. Since cryptographic research frequently benefits from the contributions of amateur cryptographers, it is important that this provision should not apply merely to bona-fide academics, but to anyone publishing information in the furtherance of research into cryptography.

It will be necessary to define what is meant by academic research, and define the conditions under which such research can be published. The DMCA provides an example of the sort of language that might be used [5]; it defines "encryption research", lists the permissible acts, and lists the factors to be considered in determining exemption, including whether any information published was published in a manner "reasonably calculated to advance the state of knowledge or development of encryption technology" and whether the person publishing it has the credentials of a cryptographic researcher (provision appears to be made for the case where the person is not actually an academic, but is merely sufficiently trained or experienced in the field).

It is clear from Professor Felten's experience that the mere existence of these clauses in the DMCA was not sufficient to prevent his being threatened with legal action. However, the subsequent climb-down by the RIAA, and the assurances obtained from the US government that "scientists attempting to study access control technologies are not subject to the DMCA"[6] appear to indicate that the DMCA's exemptions for academic research are effective[7]. The Patent Office must ensure that provisions at least equally effective appear in the UK Implementation of the Directive.

[4] See http://www.cs.princeton.edu/sip/sdmi/ for further details

[5] See Section 1201 subsection (g) of Title 17 of the United States Code: http://www.title17.com/contentStatute/chpt12/sec1201.html

[6] q.v. EFF Press release on the dropping of the Felten v. RIAA case: http://www.eff.org/IP/DMCA/Felten_v_RIAA/20020206_eff_felten_pr.html

[7] See also Declan McCullagh's article "Debunking DMCA Myths" http://news.com.com/2010-12-950229.html?tag=fd_lede

3 Effect on the common practices of professional music studios

By their very nature, copy-protection measures can be a significant inconvenience to professional music studios. The process of creating legitimate recordings frequently involves the copying of tracks from a variety of sources; any technology which prevents that copying must necessarily be avoided or circumvented.

A good example is the Serial Copy Management System (SCMS), used on digital audio recordings to control the number of generations of copies that may be made from a digital recording. Mini-disc and DAT recorders check for the presence of SCMS on incoming digital data and allow at most one generation of recordings to be made from a digital source. Attempts to make copies of these recordings will be denied.

SCMS is routinely circumvented by music professionals, and many professional DAT drives are sold with features enabling SCMS to be enabled and disabled as required. There can be no doubt that SCMS is a "technology ... which is intended, in the course of its normal operation to protect a copyright work other than a computer program"[8], that qualifies as effective since it is a "copy control mechanism, which achieves the intended protection". Consequently, anyone who circumvents SCMS is liable to civil prosecution under 296ZA, and anyone selling devices to circumvent SCMS, or possessing them "in the course of a business" is liable to civil prosecution under 296ZC and criminal prosecution under 296ZB.

The only way in which professional music studios possessing DAT drives that can circumvent SCMS and companies selling such drives can hope to escape prosecution is if they can argue that such drives are not "primarily designed, produced, or adapted for the purpose of enabling or facilitating the circumvention of effective technological measures". Now, the drives themselves clearly have other purposes, but if the mere possession of other purposes were sufficient to prevent prosecution under 296ZB/C, then any company could offer mini-disc players that circumvented SCMS to the general public without fear of prosecution, which clearly goes against the intent of the legislation. Furthermore, whilst the drives themselves have other legitimate uses, that part of them which circumvents SCMS is clearly a component (in essence not dissimilar to the mod chips applied to DVD drives to enable multi-region playback), which has no purpose other than circumvention. It is therefore not at all clear that this is a line of argument that would win in the courts (again, if it were, then anyone wishing to sell software to circumvent copy-protection mechanisms on CDs need merely incorporate into some larger piece of software with legitimate purposes (such as a combined CD/MP3 player like Winamp[9])).

It may be possible to argue that since these drives are designed for professional use (and have price tags to match), that they are unlikely to be used by those other than trusted businesses that won't engage in wilful copyright infringement, and that they don't present a threat. However, there are no get-out clauses in the Proposal that might enable the use of such an argument.

The existing section 296 of the Copyright Design and Patents Act 1988 forbids the sale of devices that circumvent copy-protection mechanism, but provides only civil remedies. Those selling equipment to music studios have nothing to fear at present, then, since it is most unlikely that a rightsholder would have reason (or the desire) to bring a case against them. Possession in the course of a business is similarly not covered by the 296 as it stands, so the studios themselves are currently safe.

Although SCMS has been used extensively as an example, above, it is not the only technical protection measure that music studios, broadcasters and others might legitimately need to circumvent in order to conduct their business. The various copy-protection techniques currently being applied to CDs are another example, and it is certain that other technological measures will be used in the future. As with SCMS, devices incorporating mechanisms to circumvent these new measures will be sold to the studios, but unless the Proposal is changed, both the studios and the manufacturers will be criminally liable.

3.1 Recommended solutions

It seems imperative, therefore, that professional music studios, other users of such drives, and manufacturers of them, should request that the Patent Office include clarifying language in the implementation so that they may be assured of freedom from prosecution.

[8] Proposal 296ZD

[9] Q.v. http://www.winamp.com/

One option is to remove section 296ZB altogether. This would revert the manufacture, sale, possession, etc. of circumvention devices to a civil offence, and leave the music studios in the same position as they are presently. There is nothing in the Directive that requires criminal sanctions for the manufacture (et al) of circumvention devices, so compliance would not be affected.

Strictly, this might not be sufficient, however, since a rightsholder in dispute for some other reason with a studio could still sue (and stand every chance of winning) under 296ZA. An exception that permits studios to circumvent, to possess circumvention devices, and that permits manufacturers to sell such devices to studios would be the preferred solution; if the criminal sanctions in 296ZB remain in force, it is the only solution.

4 Effect on beneficiaries of exceptions

In regard to article 6.4 of the Directive, the Proposal[10] enables beneficiaries of exceptions under articles 5.2(a), 2(b), 2(c), 2(d), 2(e), 3(a), 3(b) or 3(e) of the Directive to appeal to the Secretary of State where a technological measure prevents them from benefiting from these exceptions. The Secretary of State may then issue directions enabling the complainant to benefit from the exception or exceptions concerned, although he is not obliged to do so.

It appears that the Patent Office believes that it will rarely be the case that such an appeal will be necessary; unfortunately, a closer examination of the exceptions concerned reveals that the intended beneficiaries may often need to make such an appeal. In practice, the appeals process is likely to prove an unsatisfactory solution both for the beneficiary, and for the Secretary of State (or his department) who may expect to receive a very large number of such appeals.

Consider, for example, beneficiaries under article 5.3(a), namely those making copies for the purpose of illustration for teaching or scientific research. Such people might include university lecturers or schoolteachers teaching music, who wish to make copies of short sections of pieces of music for comparison in class. Where the music concerned is only offered on CDs protected by a copy-protection system, they will have no recourse but to appeal to the Secretary of State on each occasion that they need to make a copy from a copy-protected CD. There are thousands of such people across the UK, who might reasonably be expected (especially as the use of copy-protection on CDs increases) to need to make use of their exception at least once a month. It can be neither a reasonable use of their time, nor the Secretary of State's, for them to have to go through the appeals process every time they need to make such a copy.

Librarians and archivists are similarly impeded, if they must appeal to the Secretary of State on every occasion that they need to reproduce a copy of a work protected by some copy-protection system. Archivists might expect to need to do this on receipt of practically every copy-protected work they receive, since they will need to ensure that they have an unprotected copy that will remain accessible once the work passes out of copyright.

Article 5(2)(d) is an exception for "ephemeral recordings of works made by broadcasting organisations by means of their own facilities and for their own broadcasts". It would seem that this might be intended to cover such activities as creating MP3 playlists (which are easier for a radio show's DJ to control than racks of CDs; it is standard practice in many radio stations to copy CDs to MP3 to allow the DJ to switch between them more quickly and easily). It surely cannot be the case that the Patent Office intends a broadcaster to appeal to the Secretary of State on each occasion that he needs to circumvent the copy-protection on a CD in order to rip it to MP3?

Similar examples could be provided in respect of each of the other exceptions, but there is no need to do so- the point is made that the acts covered by the exceptions occur sufficiently frequently that an appeals process involving the Secretary of State is an entirely impractical approach to making the exceptions available.

[10] See section 5.2 entitled "Article 6.4" of the Proposal

4.1 Recommended solution

The exceptions listed in recital XXX should be made available by statutory legislation that obliges rightsholders to provide beneficiaries with the means necessary to benefit from the exception[11]. As it stands, the Proposal allows rightsholders to sit back and wait for complaints to the Secretary of State before they make any efforts to provide content in a suitable form to beneficiaries.

Under the Proposal, a rightsholder refusing to comply with a direction from the Secretary of State commits an actionable breach of duty to the complainant. In the revised proposal, it should be an actionable breach of duty for a rightsholder to fail to make available some means of benefiting from an an exception to the beneficiary; there should be no need to appeal to the Secretary of State first. This change enables any disputes to be resolved directly in the courts, without the unnecessary complexity (and inevitable delays) associated with involving the Secretary of State.

5 Effect on software development

Under sections 50B and 296A of the existing Copyright, Design and Patents Act 1988, reverse-engineering (decompilation) of copyrighted software programs is permitted in order to produce an interoperable product. It does not appear that either of these sections will apply to works to which technological measures have been applied (or, in as much as they do apply, they do not trump the anti-circumvention provisions of the Proposals sections 296, 296ZA, 296ZB, and 296ZC).

The implication is that reverse-engineering of a technological measure in order to create a product interoperable with some other piece of software that uses file formats protected by a technological measure, or which is itself protected by a technological measure, will not be permitted once the UK implementation is enacted. In consequence, software companies will be able to use technological measures to prevent third party developers producing products interoperable with their own.

For example, let us say that company A produces a word-processor which saves its documents using a format incorporating a technological measure, and company B wishes to produce a product that will allow authorised people to convert documents created using A's wordprocessor into one or more different formats. "Authorised people" here refers to the creators or owners of the original document, or people allowed to make copies of them. In order to write its software, Company B will need to reverse-engineer, and hence circumvent, the copy-protection applied to A's format. Even though company B may take pains to ensure that its software cannot be used to create infringing copies of documents protected by the technological measure used in A's format, it may be sued by Company A under section 296ZA for circumventing the measure. Company A might choose to do this if it were thinking of releasing a similar product later, and wished to keep the market for such conversion utilities to itself.

The proposed amendments thereby enable a software company to exert complete control over the creation of those interoperable products that can only be created with knowledge obtained from decompilation of their programs. This appears to be an unintended consequence of the proposal, since there is no language within it that seeks to justify such a dramatic change in the legality of reverse-engineering. The dangers are serious, particularly for the UK software industry, whose members are frequently obliged to write software interoperable with "standard" software written in the USA. There can be little doubt that unless provision is made to legalise decompilation of software and file formats protected by technological measures, companies will abuse the anti-circumvention provisions to erect formidable barriers against anyone seeking to write software interoperable with their own.

Whilst it is usually beneficial to a company to permit the development of other programs compatible with its own, in order to benefit from network externalities, companies with a dominant position in the market may obtain relatively little benefit from the network effect, but may be keen to prevent others from entering their marketplace. In America, the DMCA has already been used by Sony to demand that a programmer releasing open source code for the Aibo robotic dog remove the code from his website, on the grounds that to write the

[11] "The means necessary to benefit" may take any appropriate form - a rightsholder could supply a beneficiary with an unprotected copy, or some software which enables the beneficiary to make unprotected copies from the protected work, for example; the particular form doesn't matter, so long as it is easily available, and preferably advertised in such a fashion that a beneficiary can easily find out how to apply for it.

code he had to circumvent their copy-protection mechanism; although Sony eventually backed down after much protest from Aibo owners, they reserved the right to use the DMCA in a similar fashion in future[12].

5.1 Recommended solution

Amendments to the Copyright, Design and Patents Act should be introduced as and where necessary to ensure that the anti-circumvention provisions (296, 296ZA, 296ZB and 296ZC) do not in any way prevent the decompilation of computer programs as currently permitted by sections 50B and 296A of the act.

6 Expiry of Copyright

Copyright is a limited monopoly; limited by degree through the concept of fair dealing, and by extent through being granted for a limited time only. The application of technological measures to a work has the potential to move the acts permitted in respect of that work from the domain of legal control, to the domain of control exercised by the rightsholder. To prevent this, the Directive, and hence the Proposal, provide exceptions designed to allow those permitted to perform certain acts to perform them despite any use of technological measures; thus fair dealing is returned to the legal domain. However, nothing in the Proposal appears designed to ensure that a work in which copyright has expired is made available to the public in an unprotected form.

Ordinarily, the moment copyright in a work expires, it enters the public domain, and anyone may reproduce it as they wish. When it is protected by a technological measure, however, this cannot happen until either the measure has been circumvented, or an unprotected copy of the work is found. Since circumvention of the measures applied may be difficult or impossible, and since the original rightsholder may no longer exist when copyright expires, the Patent Office should consider obliging rightsholders who distribute their works using technological measures to make unprotected copies available to archivists who may then release the copies publicly on expiry of copyright.

7 Conclusion

As it stands, the UK implementation of the European Copyright Directive will hinder research into cryptography (in contravention of the express intent of the Directive itself), make criminal current common practices of the music industry, give software companies unwarranted control over the creation of software products interoperable with their own, and provide an inadequate and entirely impractical mechanism for beneficiaries of the Directive's exceptions to obtain access to copyrighted works protected by technological measures. In addition, it provides no clear mechanism for ensuring that copyrighted works protected by technological measures will eventually be released into the public domain. These problems have been explored in depth, and solutions to them proposed; it is imperative that these solutions (or others with similar effect) are adopted before the Directive is passed into UK law.

[12] See "Teaching Robot Dogs New Tricks", Scientific American, Jan 21, 2002: http://www.sciam.com/article.cfm?articleID=0005510C-EABD-1CD6-B4A8809EC588EEDF&pageNumber=1&catID=4