International Journal of Law and Information Technology, Vol. 7 No. 1

Software Piracy and the Doris Day Syndrome: Some Legal, Ethical and Social Implications of Contemporary Conceptions of Property

JAMES COUSER*

Abstract

In this paper a number of the legal, ethical and social issues raised by our ever increasing reliance upon new technologies are considered and discussed.

The spectre of software piracy is examined, along with its relationship to the criminal offence of theft, and the difficulties of ascribing the label 'thief' to those who engage in such conduct are addressed.

Particular attention is given to extent to which many large software programmers are, like the robber barons of old, attempting to reinvent themselves as paragons of respectability now that it is in their perceived best interests to do so.

Finally, it is suggested that our current conceptions of property are too outdated to adequately balance the competing issues at stake between that information which can legitimately be owned outright, that which can be

* I would like to acknowledge the guidance provided to me by Professor R.A.A. McCall Smith of the University of Edinburgh whilst writing this paper, and also thank Miss Catherine Cosgrave for her very helpful comments on an earlier draft. The responsibility for any errors which remain is, however, wholly mine.

owned for a given period of time, and that which should always be regarded as being in the public domain.

1 Introduction

> When I first studied international law, I was introduced to the topic of crimes under the *ius gentium*, the law of all peoples. These were crimes so heinous, with such international ramifications, that all states have both jurisdiction and obligation to stop them wherever they are found. They included slavery and genocide and, most memorably to undergraduate eyes, piracy. The professor pointed out jovially that it was only piracy of ships and planes that was condemned in this manner, not piracy of records or computer programmes. Nowadays, I would not be so sure.[1]

There can be little doubt that we live in a rapidly changing world; or that just as what was true for our parents may no longer hold true for us, so too those notions and norms that we currently view as universal may seem less so to our children; but Boyle's observation is strong stuff. Can we really say that what has hitherto tended to be the province of intellectual property should become an aspect of the *ius gentium*? Or, if a more restricted view is taken, is it still nonetheless possible to argue that such crimes[2] cannot adequately be dealt with by the framework of our criminal law as it presently stands, and that a fresh approach is needed?

Increasingly, we find ourselves encouraged by powerful organisations such as Microsoft and IBM, and regulatory bodies such as the Business Software Alliance and the Federation Against Software Theft, to regard copyright infringements as 'software piracy' or 'software theft'.[3] The message being put across by this terminology is that, whatever the strict legal position might happen to be, 'stealing' software is morally no different

---

[1] J. Boyle *Shamans, Software and Spleens* (Harvard, 1996), p.121.

[2] Even as the law presently stands, the English conception of copyright allows for both civil and criminal liability, depending upon the precise circumstances of the infringement involved. Accordingly, my use of the terms 'crime' and ' piracy' in this paper are not wholly disingenuous. Although I do accept that as labels they inevitably carry with them pejorative overtones, my intention here is not to steer the reader towards any particular prejudice, but rather to utilise relatively easy to comprehend descriptions. 'Infringement' might have proved a more neutral terminology, but this is, after all, principally a paper on the boundaries of the concept of theft, rather than the boundaries of intellectual property law.

[3] The strength of the computer industry, and in particular the *American* computer industry, should not be underestimated here. As a result of intense, and doubtless highly expensive, lobbying by the Software Action Group Europe – which represents such household American names as IBM, Microsoft, Apple and Digital Equipment Corporation – a 1989 Brussels directive dictated that the copyright laws of member states should be amended to extend complete protection to all software. Such a wholesale extension of the existing law was only prevented when the European Committee for Interoperable Systems – formed by European computer companies such as Olivetti, Bull and Nokia – lobbied for a less stringent system of copyright which would not have the effect of further tightening the American stranglehold over the software industry; see:– *Computer Ethics* (1994), T. Forester and P. Morrison, p. 65.

to stealing the computer on which to make use of it. The question I will attempt to address in this paper is whether that is correct, and if it is what, if any, implications this has for the criminal law in this area.

2 The Problem of Software Theft

Perhaps one of the most surprising ethical aspects of software theft is that it breaches what is described as the 'Hacker Ethic'. This holds '*that system cracking for fun and exploitation is ethically acceptable as long as the cracker commits no theft, vandalism or breach of confidentiality.*'[4] It seems that, whereas familiarity might normally be expected to breed contempt, amongst computer-users it is those who are perceived as possessing at least some degree of expertise who are most aware of the need to respect the property rights of others.[5]

However this assumes that a software program may properly form the basis of a charge of theft but, as we shall see, whilst in other areas the law has recognised the force of the sentiment that '*what is worth copying is prima facie worth protecting*',[6] the manner in which that protection is provided does not encompass *S.1 of the Theft Act 1968.* In England and Wales the offence of theft is defined in the following terms:

> A person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it; and 'thief' and 'steal' shall be construed accordingly.[7]

One of the difficulties with attempting to apply this definition to the phenomena of software piracy lies in the requirement of permanent deprivation. Whilst the old common law notion that there must be a 'taking and carrying away', preserved in the definition of simple larceny provided by *S.1(2) Larceny Act 1916,* was dispensed with by the *1968 Act* and the case law that followed on from it, it still remains the case that the owner must be deprived of their property in some way or another.

---

[4] *The New Hacker's Dictionary* (1993), E. Raymond.

[5] This is a complex issue in itself. There can be little doubt that in many of the recorded cases on the subject the hackers' motivations were not – or at the very least it was *claimed* that they were not – malicious; see:– *R v Gold* [1988] 2 WLR 984 (investigative journalism) or the American case of *Morris* ('Benign Nature of Crime Spares Hacker from Prison', B. Brock, *The Australian*, 8/5/90). However, research conducted on business students indicates that *'students who tended to use computers more are more likely to pirate software.*' (see:– 'Toward a Profile of Student Software Piraters', R. Sims, H. Cheng and H. Teegen (1996) *15 J. of Bus. Ethics 839, 846.* Of course it may simply be the case that those engaged in such a socially dubious practice as hacking are unable to live up even to the ethical norms that they set themselves, despite recognising their worth and perhaps even aspiring to them.

[6] *University of London Press v University Tutorial Press* [1916] 2 Ch. 601, 610, per Peterson J.

[7] S.1(1) Theft Act 1968.

The problem here, of course, is that it is difficult to identify what the owner of the software can be said to have lost. He still has the computer program which has been copied, and his use and enjoyment of it will have been in no way impaired by the copying process; indeed, computer operating software is designed in such a way that piracy is both simple and efficient to achieve. It represents an integral part of what it is that computers do. If I take a software programmer's umbrella from his office then he is deprived of its use – if it rains, he gets wet; but if I simply take a copy of a piece of software written by him, what can we honestly say that he has been deprived of? He still has the program in its original condition, and his ability to make use of it will have been in no way diminished by the copying process. He may well even be oblivious to his 'loss', if such it should be termed. True enough I may have interfered with his economic interests but that is not theft in these circumstances; if it were the prisons would be full of businessmen.

Arguably this represents a troubling lacuna in our conception of theft, and there are analogies that may be drawn here with what are sometimes referred to as the 'borrowing' cases. If I take a software programmer's umbrella that may be theft, but if my intention all along is to return it to him once it has stopped raining then there is no intention to permanently deprive and, *ergo*, no theft. Yet, just as my decision to borrow his umbrella may have an adverse effect upon him, so too my decision to pirate his software rather than pay for it may be said to produce consequences which, from a Kantian perspective, I am morally responsible for. I have intervened in the causal world and, in so doing, I am saddled with the moral consequences of my actions.

In the example cited before of my software programmer, if I would have otherwise had to buy his program then my decision to pirate it instead has the effect of allowing me to avoid paying the purchase price to him. I would suggest that it is a relatively uncontroversial economic truism that if *x* withholds £100 from *y*, then *y* has £100 less than would have otherwise been the case. It seems, then, that we can say that moral approbation may attach to the actions of the software pirate in these circumstances, but can we also say that it *should* so attach and, if we can, should it then also be criminalized?

3 Borrowing as Theft

At the heart of this discussion lies the distinction between actively depriving another permanently of something tangible and 'merely' withholding some benefit from them, and it is here that the 'borrowing' cases are at their most clearly analogous. My software programmer's umbrella is not an ornament or an investment, its value to him lies in its ability to keep him dry, and the fact that it is returned to him once the rain has passed is likely to do little to assuage the anger he feels. In addition to his ownership of the

umbrella as a thing, a *res corporalis*, he also owns a bundle of rights, of *res incorporales*,[8] over it, and it is these rights that have been interfered with and prejudiced.[9]

This aspect of ownership, ignored by the Criminal Law Revision Committee in their draft bill,[10] was addressed by the government of the day with the insertion of a clause that, following extensive amendment, became *S.6 of the Theft Act 1968*:

> A person appropriating property belonging to another without meaning the other to lose the thing itself is nevertheless to be regarded as having the intention of permanently depriving the other of it if his intention is to treat the thing as his own to dispose of regardless of the other's rights, and a borrowing or lending of it may amount to so treating it if, but only if, the borrowing or lending is for a period and in circumstances making it equivalent to an outright taking or disposal.[11]

This approach may have appeared to provide a solution to the perceived problem of those who would attempt to argue that they intended to return the taken property at some future point in time, yet it is of little help where the question of software piracy is concerned. The compromise effected by *S.6(1) of the 1968 Act* is to permit a finding of constructive intention to permanently deprive, rather than recognising the *res incorporalis* aspect of property ownership. That this is the case is perhaps best illustrated by the decision in *R v Lloyd*[12] in which a cinema projectionist conspired with others to remove feature films from his place of work in order to allow them to be copied and pirated. The result of Lloyd's actions were, as he was presumably aware that they would be, that the economic interests of both the copyright holder and his employer were adversely affected, and yet no one was permanently deprived of the films in question. Indeed, as Lord Lane CJ observed,

> The process of copying was done rapidly. The films were only out of the cinema and out of the hands of Lloyd for a few hours and were always back in time for their projection to take place at the advertised times to those people who attended the cinema to see them.

---

[8] *'Res corporales* are according to the legal definition physical things which can be touched; and *res incorporales* are things which do not admit of being handled, but consist in jure, and so are more properly rights than subjects .... All rights therefore are incorporeal.' See:– *Burghead Harbour Co. v George* (1906) 8 F 982, per Lord Kinnear.

[9] These issues are well discussed in 'Owning Rights and Things', G. *Gretton* (1997) 8(2) Stellenbosch Law Review Regstydskrif 176.

[10] Criminal Law Revision Committee, Eighth Report, *'Theft and Related Offences'* (1966), Cmnd. 2977.

[11] *S.6(1) Theft Act 1968*; *S.6(2) of the 1968 Act* deals with the problem of those who part with another's property under a condition as to its return – for example, where instead of borrowing the software programmer's umbrella for the duration of a storm, I pawn it for some alternative period of time – and is accordingly not relevant to the discussion at hand.

[12] *R v Lloyd* [1985] 2 All ER 661.

> It was important that the film should be returned rapidly, because if it was not it would soon become apparent that the film had been illegally removed and steps would be taken to prevent a recurrence.[13]

The question before the court was whether, notwithstanding the intention to return the films, Lloyd's actions could amount to a constructive intention to permanently deprive pursuant to *S.6(1) of the 1968 Act*. The answer given, simply, was that it could not: '*Borrowing is ex hypothesi not something which is done with an intention permanently to deprive*'.[14] Considering the phenomena of software piracy, it seems clear that if removing something for a few hours will not amount to a constructive intention to permanently deprive, then not removing it all can hardly be a more culpable act.

It is sometimes suggested that what *S.6(1) of the 1968 Act* strikes at is those situations where, having borrowed something, the defendant has used up all of the value or virtue in the item. The rogue who borrows a football season ticket intending to return it only once it has expired is but the most obvious example. However, the difficulty with this approach is that so viewed *S.6(1)* assumes a decidedly binary aspect because, as Professor Smith observes, if the life of the season ticket is viewed as a continuum then the problem of exactly where on this continuum liability for theft should be imposed '*suggests that it should not be theft of the ticket unless D intends to keep it until it has lost all its virtue*'.[15]

Legally this may well be correct, but the black or white morality which it presupposes of a world in which a borrowing is either wholly supportable or wholly insupportable seems to me to take little account of the complexities of the modern computer age in which we live.

Furthermore, attempts to unravel the Gordian Knot of *S.6(1) of the 1968 Act* by arguing that, for instance, '*the right to see each match is a separate thing in action, of which P is permanently deprived once that match is over*',[16] whilst undoubtedly ingenious, display an insufficient regard to the extent to which the nature of property ownership rights have irrevocably altered even over such a relatively short period as the past thirty years.[17]

---

[13] *Ibid*, 663.

[14] *Ibid*, 667.

[15] *The Law of Theft* (1997), J. Smith, para. 2-135.

[16] *Ibid*, fn.1.

[17] In fact this analysis may also not be entirely satisfactory under a more traditional analysis of property ownership as, if instead of it being a season ticket for Nottingham Forest which is borrowed, it is a railway travelcard this solution would implicitly result in P having been simultaneously deprived of an enormous amount of individual things in action, many of which it would have been physically impossible for him to have availed himself of as, obviously, he can only travel on one train at a time. Whilst it would be possible to rationalise this by arguing that P was deprived of the *opportunity* to take these journeys had he wished to do so, this strikes me as being somewhat artificial because, as we shall see, the *1968 Act* protects property, and not rights over or rights which are ancillary to property, and the property in this example is the season ticket itself and not the journeys it facilitates.

However, it is possible to argue that even though *S.6(1)*, as a statutory enactment, is binding upon English courts, its worth as what is sometimes rather euphemistically referred to as 'good law' is limited in the extreme. In the course of his judgement in *Lloyd*, Lord Lane CJ[18] adopted Professor Spencer's condemnation of this provision as being a section which '*sprouts obscurities at every phrase*',[19] and went on to endorse Professor Griew's view[20] '*that S.6 should be referred to in exceptional cases only.*'[21] Notwithstanding the Court of Appeal's later suggestion that the restrictive approach to *S.6* in *Lloyd* was *obiter*[22] and that the section '*is to be given its ordinary meaning (whatever that may be)*',[23] it is tempting to argue that the requirement of an intention to permanently deprive as an ingredient of theft is outmoded and anachronistic.

The problem, as has already been adverted to, is that our whole conception of what ownership amounts to has changed, and attempting to rationalise theft by reference to the old legal order is doomed to failure. The judiciary, having looked in vain to the legislature for a new legal framework capable of taking account of these changes, have attempted to resolve these difficulties but the solutions they have arrived at are piecemeal and, all to often, isolated.

Even if a more coherent approach could be discerned for this aspect of the problem, it would do nothing to address the wider issues raised by new technology. For instance, it would be perfectly possible to resolve this point without running the risk of criminalizing all borrowings, no matter how minor, by an alternative rule that held that where an intention to permanently deprive cannot categorically be demonstrated, a borrowing will still amount to theft if its net effect is to remove a *significant* element of the property's virtue. The question of what is significant would in all cases be a question of fact judged in relation to the original value of the property in question, and not the victim's resources with, as ever, the benefit of any doubt being given to the defendant. However, whilst such an approach might provide a more satisfactory method of resolving cases such as the borrowed season ticket or umbrella, it would still offer no solution to the problem of software piracy where the victim is never physically deprived of anything. Software is, in effect, information and quite aside from the separate issue of whether an intention to permanently deprive can be demonstrated or not, the law has been reluctant to hold that information can constitute property for the purposes of theft.

---

[18] *Supra* n.12, 665.
[19] See:– 'The Metamorphosis of Section 6 of the Theft Act', J. *Spencer* [1977] Crim.LR 653.
[20] *Supra* n.12, 666.
[21] The Theft Acts 1968 and 1978 (1982), E. Griew, para. 2-73.
[22] *R v Bagshaw* [1988] Crim.LR 321.
[23] *Supra* n.15, para. 2-128.

4 Theft of Information: Giving Thieves a Piece of Our Minds

It was clear at common law and under the *Larceny Acts of 1861 and 1916* that the requirement that there be a taking and carrying away meant that intangible property could not be stolen.[24] However, *S.4(1) of the 1968 Act* defines 'property' as including '*money and all other property, real or personal, including things in action and other intangible property*'. This section could have been interpreted as including information but it is now clear, following the decision in *Oxford v Moss*,[25] that this is not the case.

In *Oxford v Moss* a student obtained the proof of an examination he was due to sit, thus forcing the authorities to expend time, effort and money on formulating a replacement paper. The student was charged with the theft of certain intangible property, namely the confidential information contained within the examination paper,[26] but it was held at first instance that confidential information did not fall within the definition of property contained in *S.4(1) of the 1968 Act*, and this finding was upheld on appeal.

On the one hand this could be viewed as a rogue's charter, but there are formidable objections to construing the law in any other fashion. As the Canadian House of Commons Standing Committee on Justice and Legal Affairs phrased it,

> For reasons of public policy the exclusive ownership of information which, of necessity, would flow from the concept of 'property', is not favoured in our social-legal system. Information is regarded as too valuable a commodity to have its ownership vest exclusively in any particular individual.[27]

The spirit of this passage was adopted by the English Law Commission[28] in their report into this area of the law. The problem, simply put, is that information – be it confidential or otherwise – is too abstract a concept to bring within the existing scheme of things.

Yet, just as the specific problems of the abstracting of electricity and the 'borrowing' of motorcars and pedal cycles led to the strict rules of the *Theft Act 1968* being relaxed to permit criminalization in these circumstances,[29]

---

[24] See: – *Supra* n.15, para. 2-89.

[25] *Oxford v Moss* [1979] Crim.LR 119.

[26] It was conceded that Moss never had any intention to permanently deprive the university of the paper itself because, as in *Lloyd*, returning the property before anyone became aware of its absence formed an integral aspect of his plan.

[27] Canadian House of Commons Standing Committee on Justice and Legal Affairs, *Report of the Sub-Committee on Computer Crime* (1983), p.14.

[28] Law Commission Working Paper 110.

[29] Abstracting electricity is an offence contrary to *S.13 of the 1968 Act*, whilst taking a conveyance and taking a pedal cycle are criminalized by, respectively, *Ss.12(1) and 12(5) of the 1968 Act.*

so too it was suggested that the phenomena of computer crime warranted special legislative attention. The Law Commission's response was to argue that any extension of the definition of property to include information would cause '*problems which have general implications outside the region of computer misuse*'.[30] Instead a solution of sorts was provided by the *Computer Misuse Act 1990*.

5 The 1990 Act: Treating Computerised Information Differently

The first point that should be made about the *1990 Act* is that its introduction was principally prompted by concerns about the activities of computer hackers,[31] rather than to deal with the specific problem of software theft, or for that matter the theft of confidential information. Accordingly, what application it has to the subject of this paper is necessarily tangential rather than direct. Nevertheless, it remains the case that it does have *some* application in this area. Thus, following O*xford v Moss*, whilst an individual who photocopied a document containing the source code for a computer program would not commit the offence of theft,[32] it is clear that if the program was stored on a computer to which he was not permitted access then, while copying the program itself will still not be criminalized, the unauthorised access will. *S.1(1) of the 1990 Act* provides:

A person is guilty of an offence if

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

(b) the access he intends to secure is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

From a purely utilitarian perspective this seems to provide a workable solution to many of the most morally reprehensible instances of software

[30] *Supra* n.28, para. 3-69.

[31] The straw which finally broke the camel's back in this area – the government having already reneged on its 1989 promise to Emma Nicholson MP to legislate in return for her agreement to withdraw her private member's *Anti-Hacking Bill* – was the decision by the House of Lords in *R v Gold* [1988] 2 WLR 984 that the *Forgery and Counterfeiting Act 1981* could have no application against two supposed investigative journalists who succeeded in hacking into the British Telecom Prestel Gold computer network and engaging in such mischief as leaving a message in the Duke of Edinburgh's computerised mail system which apparently read 'GOOD AFTERNOON. HRH DUKE OF EDINBURGH'. The prosecution's submissions in this case were described in the Court of Appeal as a *'Procrustean attempt to force these facts into the language of an Act not designed to fit them'*; *R v Gold* [1987] 3 WLR 803 per Lord Lane CJ.

[32] Assuming, for the sake of argument, that he used his own photocopying machine and paper.

piracy. True enough, it can have no application against the individual who obtains a copy of a software program through legitimate channels and then proceeds to pirate it using her own computer, but it does deal with those who commit the computer equivalents of trespass or burglary,[33] the immorality of which may be so great as to warrant special attention. As the Republican Congressman Ed Zschau observed when his Capitol Hill computer was hacked into and his records tampered with,

> The entering of my computer was tantamount to someone breaking in to my office, taking my files and burning them … the police would be more concerned if this were a physical break-in. Because people don't see the files overturned or a pile of ashes outside the door, it doesn't seem as bad … But it is equally devastating.[34]

Yet, emotive as this issue undoubtedly has the potential to be, the solution effected by *S.1 of the 1990 Act* is not to my mind a satisfactory one. In its initial report the Law Commission expressed reservations over the criminalization of mere unauthorised access to a computer, but altered its opinion on the matter after receiving submissions from a number of large corporations who each confirmed that even a suspicion that their computer files or programs had been tampered with 'forced' them to expend quite considerable sums of money in order to satisfy themselves of their systems' continued integrity.

This may be true, indeed one instance cited to the Law Commission involved the expenditure of no less than ten thousand man hours spent checking for evidence of sabotage, yet is this really so different to other instances where the owner of property may be placed in doubt as to its integrity, but without the imposition of liability ever being considered? The obvious example is that of the homeowner who finds that their door keys have been borrowed for two hours: they will almost inevitably feel compelled to change their locks, quite possibly at considerable expense, but surely imposing criminal liability upon the borrower is taking the concept of the inchoate offence a step or three too far? Even more to the point, from the perspective of software theft, is the instance where a financial institution fears that the written source code for its credit card encryption program may have without authorisation been viewed and memorised by some third party. This would be no offence, but copying the program from their computer would be. As Lloyd and Simpson put it:

---

[33] In fact *S.2 of the Computer Misuse Act 1990* provides an ulterior intent offence, with enhanced penalties, applicable against those who commit the *S.1* offence with intent to commit any other offence *'(a) for which the sentence is fixed by law; or (b) for which a person … may be sentenced to imprisonment for a term of five years'*, but as the ulterior offence committed would, for the purpose of this paper, be at most criminal copyright infringement which carries a maximum sentence of two years imprisonment, this section could have no application and it is not proposed to discuss it further.

[34] Congressman Ed Zschau cited in *Computer Ethics* (1994), T. Forester and P. Morrison, p.41.

> If comparison is made with other forms of property and behaviour, it will be seen that the effect of … [S.1 of the Computer Misuse Act 1990] … is to confer an exalted status upon data held in a computer system. Save under the provisions of the Official Secrets Acts, if confidential information is written on a piece of paper which is left on top of a desk visible through a window, no offence would be committed by a person who looked at the document through the window. No offence indeed would be committed by a person who took a photograph of the document and its contents … [Furthermore, a]s a general rule, the mere act of obtaining access to property does not constitute an offence. This occurs only where security measures are overcome or where property is damaged or removed.[35]

These last issues are to the point because, leaving aside the eighth data protection principle which stipulates that there must be adequate security measures where a computer contains personal information, there is no requirement under the *1990 Act* that the computers or programs that are the subject of the unauthorised access should have sufficient, or indeed any, safeguards designed to protect their integrity. This is a troubling situation for a number of reasons.

Firstly, the purpose of the *1990 Act* was to deal with the perceived problem posed by computer hackers. Yet, *S.1* in particular, is couched in such wide terms that it has the potential to criminalize vast swathes of conduct which, candidly, it is difficult to believe would have ever been in the contemplation of the draftsman. 'Computer' is not defined in the Act and '*can include equipment which has computer technology built into it although it would not normally be described as a computer*',[36] whilst securing access has been construed as including causing the computer to perform any function. As there is no requirement that any security measures should first be overcome, it seems that the unauthorised use of a washing machine, digital watch or even some of the more sophisticated hairdryers may now be punishable by six months imprisonment. Common sense on the part of prosecutorial agencies would doubtless ensure that such charges would in practice seldom, if ever, be preferred, but I would suggest that the possibility of executive discretion is no substitute for properly thought through coherent legislation.

Furthermore, by criminalizing mere unauthorised access, the effect of *S.1. of the 1990 Act* is to punish activities which are themselves not the conduct that is considered to be morally reprehensible. Where a competitor left unattended in my software programmer's office makes unauthorised use of the software programmer's computer to pirate some or all of his latest software, it is not the use to which he puts the keyboard

---

[35] I. Lloyd and M. Simpson *Law on the Electronic Frontier* (1994), Edinburgh University Press pp.22/23.
[36] Introduction to Computer Law (1996), D. Bainbridge, pp.250/251.

and hard drive which is objectionable because '*this is a purely incidental aspect of the crime – like getaway drivers that break speed limits after having robbed a bank*'.[37] Yet in the eyes of the *1990 Act* the competitor is legally no more culpable than if he had used the computer to play 'Minesweeper' or, for that matter, blow dry his hair or wash his socks. Such a provision may be effective, but that of itself does not make it any less objectionable.

Professor Smith identifies the problem as being

> … should we produce new, purpose built legislation, or should we pretend that the computer simply affords us new ways of committing the oldest wrongs, and expect the judges to mould the old law on our behalf?[38]

It is clear from the tone of this passage which of these alternatives Smith himself favours[39] but, as we have seen, simply attempting to utilise legislation to deal with perceived shortcomings in the existing law is a less than satisfactory answer to the problem. Might the solution be to 'mould the old law' to meet this new challenge?

6 Confidential Information as Property: The Canadian Approach

The Divisional Court's decision in *Oxford v Moss* was not fully reported and so it is not possible to say categorically if the question of whether information should be construed as property was afforded a particularly considered hearing. However, the Canadian case of *R v Stewart* was reported fully at all levels and, although ultimately the outcome was the same, the Court of Appeal at least considered that some forms of information could be the subject of a charge of theft, contrary to *S.283 of the Criminal Code*, which provides that,

> Everyone commits theft who fraudulently or without colour of right takes, or fraudulently and without colour of right converts to his use or the use of another person, anything[40] whether animate or inanimate.

The allegation against Stewart was that, on behalf of a trade union who

---

[37] *Digital Crime* (1997), N. Barrett, p.67.

[38] 'Computer Crime: A Reply' A. T. H. Smith *(1987) 3 Yearbook of Law, Computers and Technology 204, 205.*

[39] Indeed, Smith goes on to observe – correctly in my opinion – that 'As judges struggle with the old law, we cannot be sure that they can be clear about the sorts of interests that they ought to be seeking to protect'; See:– *Ibid.*

[40] Despite the use of the word 'anything' in this section it was conceded at all levels that this had to be interpreted as meaning 'any property'; See:– *Information Technology Law* (Butterworths, 1993), I. Lloyd, para. 16-20.

were hoping to recruit new members, he attempted to obtain the personnel details of a hotel's employees from its computer system. At first instance Stewart was acquitted by the trial judge, Krever J., who held that,

> … confidential information is not property for the purpose of the law of theft in Canada… If this interpretation should be thought to be inadequate to meet the needs of modern Canadian society, particularly because of its implications for the computer age, the remedy must be a change in the law by Parliament. It is not for a court to stretch the language used in a statute dealing with the criminal law, to solve problems outside the contemplation of the statute. If an accused person's conduct does not fall within the language used by Parliament, no matter how reprehensible it might be, it ought not to be characterised as criminal.[41]

In the Court of Appeal, however, the majority took the view that, at the very least, confidential information would fall within the ambit of *S.283*, on the basis that such protection was appropriate for '*confidential information which has been gathered through the expenditure of time, effort and money by a commercial enterprise for the purpose of its business*'.[42] As has already been adverted to, this decision was overturned by the Supreme Court[43] following considerable criticism of the Court of Appeal's decision, but that is not to say that the question of whether confidential information *should* constitute property has been categorically laid to rest and it is worth rehearsing the arguments for and against briefly at this juncture.

Doherty's reasons for agreeing with the Court of Appeal's approach are perhaps best summed up by simply citing the title of his paper: '*Stewart: When is a Thief not a Thief? When he Steals the Candy but not the Wrapper*'.[44] This is a view with some merit and, from the point of view of software piracy, more than just a little relevance. What matters to the programmer who has spent six months creating a piece of software is not that he has been deprived – permanently or otherwise – of a £1 floppy disk, but rather that he has lost the fruit of his labour. It is here, however, that the flaw in this argument becomes apparent.

As we have already seen, the programmer has *not* been deprived of his work, rather he has had its exclusivity removed. His economic interests have been adversely interfered with, but the information – the knowledge – which was previously his exclusively has not disappeared into the ether, even if its practical worth to the programmer may have diminished. James Madison once observed that,

---

[41] *R v Stewart* (1982) 138 DLR (3d) 73, 85.

[42] *R v Stewart* (1983) 149 DLR (3d) 583, 595.

[43] *R v Stewart* 50 DLR (4th) 1.

[44] 'Stewart: When is a Thief not a Thief? When he Steals the Candy but not the Wrapper' G. Doherty *(1988) 63 Criminal Reports 3d 322.*

> Knowledge will ever govern ignorance; And people who mean to be their own Governors must arm themselves with the power which knowledge gives.[45]

Yet, true as that may be, the fact remains that,

> Knowledge is valuable, but knowledge is neither real nor personal property. A man with a richly stored mind is not for that reason a man of property. Authorities which relate to property in compositions belong to the law of copyright and have no bearing upon the question whether knowledge or information, as such, is property.[46]

Knowledge can truthfully be described as belonging both to everyone and to no-one, and it is this plurality of ownership which poses particular problems when the possibility of imposing liability for theft on software pirates arises.

7 Protecting Residual Interests: Intellectual Property or Crime?

Suppose that a programmer, Adam, sells a copy of his software to Beryl. If that software is later pirated by Charles, who is the victim? Under a traditional analysis of property ownership we might feel drawn to conclude that Adam disposed of any interest in the product when title to it passed to Beryl. Had he instead sold her a car which was then later taken by Charles, we would not expect the police to obtain a victim statement from Adam – or indeed the Ford Motor Company – simply because of an historical interest in the property.

Of course these difficulties are in practice circumvented by having Adam licence his product to Beryl, rather than sell it to her outright, thus enabling him to retain a residual interest in his software. However, this simply underlines the inappropriateness of attempting to fit the square peg of intellectual property rights into the round hole of theft: such licensing arrangements are creatures of the laws of copyrights and patents, not crimes. As Hammond observes,

> … in the British Commonwealth jurisdictions … protection of confidential information sounds either in contract or in equity, not

---

[45] Letter from James Madison to W.T. Barry (4th August 1822), reprinted in The Complete Madison (1953), S. Padover (ed.) p.337.

[46] *The Federal Commissioner of Taxation v United Aircraft Corporation* cited in 'Theft of Information', R. Hammond *(1984) 100 LQR 252, 253.*

> 'property'. That is, the law protects confidential relationships, and improper conduct with respect thereto.[47]

Suppose further that Adam's software program is nothing more exotic than a searchable listing of all ex-directory names, addresses and telephone numbers in a given area. Certainly that information is confidential and certainly Adam will have expended time and effort creating his program.[48] Furthermore, from the perspective of copyright protection, Adam may well have a residual interest in his work as the concept of 'originality' is hardly stringent and would be satisfied where a direct causal link between his original idea and the finished product could be demonstrated,[49] yet should we equate that residual interest with ownership as the concept of information as property would tend to suggest? Whilst it is true that in exceptional circumstances a copyright can of itself form the basis of a charge of theft,[50] the contention that the copyright subsisting in confidential personnel details could constitute property for the purposes of theft, adopted in the Court of Appeal in one of the majority judgements in *Stewart*,[51] was resoundingly and, I would suggest rightly, rejected by the Supreme Court of Canada on appeal.

Information is simply too nebulous, too malleable, to allow it to be described as property as that term is presently understood. Whilst in the context of an ex-directory listing a man's name may represent confidential information, it is nothing more than a matter of public record when recorded on his birth certificate. The information itself is unchanged but, seemingly, its status has altered. The point is well made by Lloyd and Simpson, who observe that:

> Although swords may be beaten into ploughshares, the process is a difficult one and involves destruction of the original object. The uses to which information can be put are limited only by the imagination of its possessor and the same raw material may be used for an infinite number of purposes.[52]

This is a matter of no small import for software programmers because, whilst according exclusive control over property protects its new owner, this is of necessity only achieved by curtailing any other claims to, or over, it.

---

[47] *Ibid*, 257, footnotes omitted.

[48] For the purpose of this argument I will assume that Adam came by this information legitimately, albeit that I accept that even legitimate means of obtaining such details have to be regarded as morally suspect in the extreme; See:– 'Who Owns Your Name and Address?' in *Who Owns Information? From Privacy to Public Debate* (1994), A. Branscomb, pp.9/29.

[49] See:– *University of London Press v University Tutorial Press*; *Supra* n.6. This is a considerably less onerous test to satisfy than that of 'novelty' required in patent law.

[50] See:– *Rank Film Distributors v Video Information Exchange* [1982] AC 380, 443, per Lord Wilberforce.

[51] *Supra* n.42.

[52] *Supra* n.35, p.36.

Acceptable, perhaps, where what is being considered is an umbrella, but less so surely in the case of information.

What the software industry is attempting to achieve when it appeals to the terminology of the law of theft to describe infringements of its copyrights, is the protection of innovation at the expense of future innovation. Having been the first across the river they now wish to see the bridge dismantled but, whilst the final few steps may have been theirs alone, the whole bridge is unlikely to have been assembled from scratch. Innovations to knowledge are almost invariably incremental, yet whilst the law of copyright recognises this by placing limits on the length of time that an idea may be protected, the law of theft is designed to protect property, not innovations. What is mine today is mine for all my tomorrows, but what I own is merely the thing and not the concept behind it. My software programmer's ownership of an umbrella does not provide him with an ancillary right to prevent anyone else creating a better, or a worse, or even simply a different, method of keeping the rain off of peoples' heads. The law of theft is apt to have such unwanted and unwarranted consequences.

8 Protecting Innovation or Stifling it?

This is of fundamental importance to us all. It has been suggested – and some of the more startling cases seem to bear this out – that the officials responsible for granting copyright and patent protection have too little technological knowledge to be able to differentiate between truly innovative software and mere derivation from other, unprotected, sources:

> People who owe their fame, and in some cases their fortunes, to their status as innovators – Mitch Kapor, creator of Lotus 1-2-3, Richard Stallman, the creator of GNU-Emacs – have begun to argue[53] that contemporary intellectual property rights are so broad as to slow the rate of innovation.[54]

Thus Hayes Microcomputer were granted

> … a patent on a program that simply switches a modem from transmit mode to receive mode. Hayes apparently now has exclusive rights to any program that performs the same function until the year 2002.[55]

More startlingly yet, Merrill Lynch were apparently awarded a patent over a process that facilitated the movement of funds between accounts,

---

[53] See:– 'Why Patents are Bad for Software', S. Garfinkel, R. Stallman and M. Kapor *(1991) 8 Issues in Science and Technology 50.*

[54] *Supra* n.1, p.xiii.

[55] *Computer Ethics* (1994), T. Forester and P. Morrison, p.63.

despite the Federal District Court accepting that this was simply a business process which, if done by hand, could be afforded no protection whatsoever. It seems that whoever becomes the first to reduce a process into computer code is to be treated as the owner not just of that particular process, but also of the knowledge that it relates to.

This is an alarming enough prospect even where what is being considered is the limited property status accorded to information by the law of intellectual property, but it represents a wholly unacceptable straitjacket upon the back of innovation where the absolute property interests of the law of theft are concerned. The problem, simply put, is that software programmers are torn between competing interests:

> … the large software companies have interests both in the protection of software (their own) and in a limitation on the protection of software (their competitors).[56]

This, however, is simply the status quo of power; having utilised the work of others in order to create their software, the programmers now wish to claim it – *all of it* – as theirs and theirs alone. Mitch Kapor, the creator of Lotus 1-2-3, may condemn this as anti-innovative, citing the fact that had patent protection been available to the software company which wrote the earlier, but arguably inferior, VisiCalc spreadsheet program then he would have been prevented from developing his superior product. This may be so, but it did not stop him from obtaining such protection for his product when the ambit of patent protection was extended in America, and it has not stopped him from successfully suing a number of other programmers who he considers to have copied his software. Indeed, it is not uncommon for programmers to include 'fingerprints' in their software – unique mistakes designed to catch out those who attempt to copy a program through a process of reverse engineering from the original – because, as Lloyd and Simpson observe in relation to the case of *John Richardson Computers Ltd v Flanders and Chemtec Ltd*:[57]

> It appears to be a feature of cases in this area that similarities of mistakes rather than of valuable features is more damaging to an alleged copyist.[58]

Having drawn on the work of others, they now claim that it is wrong of anyone else to do the same. This is a contention that has cultural, as well as legal, implications because whilst America was once the biggest copyright pirate of them all,[59] it now complains the most vociferously about the behaviour of those in the Third World and eastern Europe, arguing in favour of an extension of the existing law in the name of professional ethics.

---

[56] *Supra* n.1, p.159.
[57] *John Richardson Computers Ltd v Flanders and Chemtec Ltd* [1994] FSR 144.
[58] *Supra* n.35, p.75.
[59] See:– *Supra* n.1, pp.2/3.

Yet anyone can embrace ethics when it is in their perceived best interests to do so, when they have more to lose than they do to gain by not doing so, but can that truly be described as an ethical position? Having lost their ethical virginity should the likes of Bill Gates or Mitch Kapor be allowed to re-invent themselves and seize the moral high ground in order to enhance the value of their share holdings? Groucho Marx once remarked '*I've been around so long I can remember Doris Day before she was a virgin*'. Should we now say the same of those programmers who encourage us to think and speak in terms of software piracy and software theft?

In part the deeply condemnatory tone that I have adopted misrepresents my views. It is not that I am advocating deregulation or even that I am arguing that the anti-competitiveness of suppressing innovation is necessarily a bad thing.[60] There are wider societal issues at play here, and an element – even a very substantial element – of anti-competitiveness may be justifiable in order to realise the greater utilitarian goal of having computers and computer networks that are able to communicate with each other. Refrigerators that tell the supermarket when we are out of milk, cars that tell the garage that their tyres are low on air; the permutations are endless, but all presuppose compatible software which in turn presupposes a dearth of alternatives. Needless to say, this does not even begin to consider the advantages to consumers of economies of scale.[61]

These are powerful considerations, and their worth undoubtedly does warrant protection. Yet, as we have seen, the law of theft as it is presently formulated is simply too blunt an instrument to take account of the fine distinctions presented by the quandary of offering a degree of protection for computer software which is neither too onerous nor too weak. This is an issue which we will return to, but first this might be a reasonable point at which to consider what it is about the piracy of information that we find so objectionable, along with an evaluation of the effects upon information holders and information seekers of what I will term the Doris Day syndrome – the tendency to reinvent oneself in such a way as to alter not only one's own status in relation to information, but also the status of others in relation to it.

9 The Doris Day Syndrome: Ethical Implications of the Ownership of Information

Following the discovery of the Dead Sea Scrolls by Bedouin tribesmen in 1947 the International Committee to Edit the Scrolls of Cave 4 Qumran was

---

[60] Although for a strident defence of exactly such a position, see:- 'Who Owns Computer Software' in *Who Owns Information? From Privacy to Public Access* (1994), A. Branscomb, p.138, pp.151/154.

[61] These and related benefits are concisely presented *in 'Bill Gates Rules Cyberspace, OK?'*, M. Beachill, *Living Marxism No. 110 (May 1998), pp.36/37.*

established. This was comprised of seven scholars from around the world whose task it was to undertake the mammoth process of translating and collating the information contained within the Scrolls.[62] This represented more than simply the work of a few years, it was, and still is, the work of many lifetimes. Each of the scholars made a huge personal academic investment in the project, because having embarked upon their work each of them knew that it would be decades before it finally saw fruition. Indeed, some of them would reach retirement age before that day arrived, in which case their work was continued by another academic, picked by the retiring scholar and agreed by the other members of the International Committee.

Doubtless what each of these seven scholars feared the most was that someone else would pre-empt the publication of their finished research. In much the same way that a programmer may live in fear of a competitor introducing a similar piece of software first, so too these academics dreaded the prospect of reaching the summit of the mountain only to find that another had already beaten them to it. Such an outcome would mean that decades of their lives had been expended upon a project for which they would not even receive the academic credit. It is probably no exaggeration to say that it would be the most grievous injury that could possibly be inflicted upon them and, perhaps not surprisingly, their research was conducted in great secrecy. Furthermore, publication of a paper which concerns the work of a fellow academic represents a gross breach of archaeological professional ethics and is, apparently, punished by the offending academic being shunned within the international archaeological community.

> All of this is understandable; such considerable personal sacrifice surely deserves a considerable degree of protection in return. It is in everyone's – or at the very least every academic's – best interests that matters should be so arranged because preventing them from stealing another academic's thunder in turn helps to preserve the integrity of their own work. Archaeology is seemingly a co-operative and close knit community and the seven scholars engaged on the research into the Dead Sea Scrolls probably felt reasonably confident that their worst fears would never become reality. On 4th September 1991 they discovered that this was an overly optimistic hope.

From the perspective of the seven scholars, the Biblical Archaeology Society of Washington's (BAS) announcement that it intended to release a translated section of the Scrolls for general dissemination amounted to little more than academic vandalism, and there were many other archaeologists who agreed with them. Yet condemnation for the BAS's

---

[62] A fuller account of this discovery and the subsequent establishment of the International Committee to Edit the Scrolls of Cave 4 Qumran can be found in 'Who Owns Religious Information?' in *Who owns Information? From Privacy to Public Access* (1994), A. Branscomb, pp.119/137.

actions was in no way universal; far from having 'stolen' from the work of the seven scholars, the BAS's translation represented an astonishing piece of archaeological detective work and was itself arguably a substantial contribution towards the research into the Scrolls.

The secrecy surrounding the work of the seven scholars was such that few details about the Scrolls had ever been released. There were no transcripts or photographs of them in general circulation, but there was a concordance – an alphabetical listing of every single word in the Scrolls, along with the words immediately preceding and following it – and it was from this that, using an ordinary desktop computer, the BAS had succeeded in piecing together their translation as if it were a jigsaw puzzle. The seven scholars of the International Committee may have had their interests in the previously confidential information, and indeed their interests in literally decades of research, adversely interfered with but, as the BAS demonstrated, there really was no need for painstaking and time consuming reconstruction when a relatively simple computer program, coupled with the requisite archaeological expertise, could exponentially expedite matters.

Furthermore, whilst other archaeologists would have still been aware of their own self-interest in the maintenance of the ethical norm which helped to preserve the integrity of research, the seven scholars had hardly enamoured themselves by their attitude towards other academics over the previous forty years. There had been no transcripts or copies released, and the numerous requests for access to the actual Scrolls themselves had all been rebuffed out of hand. Additionally, as the scholars tended to appoint their own replacements, the noses of a large number of leading academics had, over the years, been put out of joint as they were passed over for a position on the International Committee in favour of protégés who were often perceived as being less gifted.

Most damning to the seven scholars' cause, however, was the sheer length of time that the above state of affairs had persisted. Secrecy in order to preserve academic integrity is one thing, but a forty year monopoly is something else altogether. As Dr. Lawrence Schiffman, Professor of Hebrew and Judaic Studies at New York University put it:

> Most will regard those who make this material available as Robin Hoods, stealing from the academically privileged to give to those hungry for the knowledge secreted in those texts.[63]

Whatever the ethics of their behaviour might happen to be, there can be little doubt that the BAS's actions forced a compromise out of the seven scholars. Within two months the Israeli Antiquities Authority and the

[63] Dr. Lawrence Schiffman cited in 'Monopoly Over Dead Sea Scrolls is Ended', J. Wilford, *New York Times (22/9/91), p.A.20.*

International Committee reversed their previous positions and began allowing other academics access to sections of the Scrolls in return for an undertaking of non-publication. Furthermore, translations of various passages began to become generally available, and this should in no way be viewed as mere serendipity – something that would have in any case occurred at that time. It was a compromise, not a total surrender, that was reached, and there are still numerous sections of the Scrolls that may be viewed only by the Members of the International Committee.

We can see, then, that both the seven scholars and the BAS occupy positions that are capable of defence, but that by focusing solely upon their own internalised goals each fails to see the 'bigger picture' and succeeds principally in alienating the other. The seven scholars failed to take account of the academic needs of other archaeologists, and ignored the dynamic effects which a fresh approach to an old problem frequently can deliver, whilst the BAS drove a coach and horses through the ethical principle of non-publication – having obtained their translation they could have attempted to negotiate with the International Committee in order to 'force' them into early publication, instead of publishing and claiming the kudos for themselves.

This is in many ways analogous with the polarised positions of the software industry and at least some of those who support piracy. The large corporations are wont to paint a picture of the software pirate as the unscrupulous trader – almost certainly from the Third World or the old Soviet Union – who produces counterfeit versions of their products from which he derives vast profits at their expense. Such individuals undoubtedly do exist but that is not the whole picture, and so whilst there are a number of startling instances of large organisations which frankly ought to have known better engaging in the wholesale piracy of software, there are also those individuals who on moral grounds object to the idea that information may be owned. The question becomes can a genuinely held conviction that a given course of action is right vindicate the actor's conduct? It is apt that, in the passage cited earlier, Dr. Lawrence Schiffman described the BAS as 'Robin Hoods' because, in discussions regarding criminal liability, this argument is known as the Robin Hood defence to dishonesty.[64]

10 If Software Pirates are Robin Hoods, Who's the Sheriff of Nottingham?

The *1968 Act* does not define what it means by 'dishonesty' with any great precision as the Criminal Law Revision Committee expressed the view that, much like the proverbial elephant, '*'Dishonesty' is something which laymen can*

[64] See:– 'Dishonesty in Theft: A Dispensable Concept', D. Elliot *[1982] Crim.LR 395.*

easily recognise when they see it.'[65] However, the Act does contain two provisions which offer some degree of guidance. *S.1(2) of the 1968 Act* provides that,

> It is immaterial whether the appropriation is made with a view to gain, or is made for the thief's own benefit

Whilst *S.2 of the 1968 Act* identifies three examples of what is not dishonest, and one example of what may be:

> (1) A person's appropriation of property belonging to another is not to be regarded as dishonest –
>
> (a) if he appropriates the property in the belief that he has in law the right to deprive the other of it, on behalf of himself or of a third person; or
>
> (b) if he appropriates the property in the belief that he would have the other's consent if the other knew of the appropriation and the circumstances of it; or
>
> (c) (except where the property came to him as trustee or personal representative) if he appropriates the property in the belief that the person to whom the property belongs cannot be discovered by taking reasonable steps.
>
> (2) A person's appropriation of property belonging to another may be dishonest notwithstanding that he is willing to pay for the property.

S.1(2) would seem to dispose of the software pirate who seeks to rely upon a Robin Hood defence by arguing in favour of the sanctity of information. The individual who posts software onto an internet bulletin board with the intention that others should download it for free may obtain no tangible benefit beyond a sense of warmth in his heart at having facilitated the free flow of information but, so says the *1968 Act*, it is not his gain but rather the victim's loss which renders a particular set of circumstances dishonest. Yet, as we have seen, *S.2* mitigates any strictness which this might have engendered and it is instructive to consider the ways in which this has been construed.

At common law it is clear that even the strongest moral claim will not render honest that which is otherwise dishonest,[66] but whilst *S.2(1)(a) of the 1968 Act* speaks specifically of a 'right in law' this '*does not necessarily exclude a belief in a merely moral right*'[67] and it seems likely that, as the jury are now the

---

[65] *Supra* n.10, para. 39.
[66] *Southwark London Borough Council v Williams* [1971] Ch. 734, 744; *Supra* n.15, para. 2-116, fn.2.
[67] *Supra* n.15, para. 2-116.

arbiters of what is and is not dishonest,[68] the common law rule has been displaced and, for example, the jury would now be entitled to acquit the Little Match Girl had she chosen to appropriate a coat rather than freeze to death.[69]

However, whilst it is one thing to blithely identify that certain moral claims may in certain circumstances negate dishonesty, it is quite another thing altogether to formulate a test by which to separate out the deserving from the undeserving. In *R v Feely*[70] the Court of Appeal held that the question of what amounted to dishonesty was one for the jury to decide by reference to,

> … the current standards of ordinary decent people … [as i]n their own lives they have to decide what is and what is not dishonest. We can see no reason why, when in a jury box, they should require the help of a judge to tell them what amounts to dishonesty.[71]

Notwithstanding the fact that different juries may reach different conclusions about similar sets of circumstances, this is a workable enough – if somewhat utilitarian – test but, perhaps mindful of the fact that an overly objective approach might 'force' juries to convict those in the position of the Little Match Girl, the Court of Appeal upheld a jury direction given by the trial judge in the case of *R v Gilks*[72] which suggested that they '*try and place yourselves in [the defendant's] position at that time and answer the question whether in your view he thought he was acting dishonestly.*'[73] This led to a finding that Mr. Gilks had not been dishonest in keeping the money overpaid to him by a bookmaker, despite his earlier admission that such conduct would be dishonest in relation to receiving too much change from a grocer, because – apparently – bookmakers are '*a race apart*''.[74] The flaws in this approach are not especially difficult to discern.

Such an approach is hopelessly subjective. An individual may hold a heartfelt conviction that large multi-national software companies, such as Microsoft or Apple, are also a 'race apart', and yet that of itself should not be a sufficient excuse to dispose of the question of whether pirating their software is dishonest. It may be perfectly possible to argue, following *Gilks*, that whilst it would be dishonest to pirate software from a less well established source, the sheer wealth and resources of corporations like Microsoft and Apple renders them 'fair game', but as Professor Williams pointed out:

---

[68] Infra n.76 and accompanying discussion.

[69] Even at common law this could perhaps be viewed as an example of the newly 'discovered' defence of duress of circumstances; See:– *R v Conway* [1988] 3 All ER 1025.

[70] *R v Feely* [1973] 1 All ER 341.

[71] *Ibid*, 345, per Lawton LJ.

[72] *R v Gilks* [1972] 3 All ER 280.

[73] *Ibid*, 283 per K. Bruce Campbell Esq. QC cited by Cairns LJ.

[74] *Ibid.*

> Subjectivism of this degree gives subjectivism a bad name. The subjective approach to criminal liability, properly understood, looks to the defendant's intention and to the facts as he believed them to be, not to his system of values.[75]

It was in response to these and aligned criticisms that the Court of Appeal took the opportunity to re-visit the concept of dishonesty in what is now the leading judgement in this area, *R v Ghosh*.[76] The test for the jury to apply is now twofold:

> (i) Was what was done dishonest according to the ordinary standards of reasonable and honest people? If no, D. is not guilty. If yes –
>
> (ii) Did the defendant realise that reasonable and honest people regard what he did as dishonest? If yes, he is guilty; if no, he is not.[77]

Lord Lane CJ was clearly of the opinion that this objective/subjective test[78] would remove any possibility of a defendant relying upon a 'Robin Hood' defence.[79] However, as Elliot points out,

> … it plainly does not do so, because he is entitled to be acquitted if the jury think either (a) that what Robin Hood did (rob the rich to feed the poor) was not dishonest or (b) that Robin Hood thought the plain man would not consider what he did as dishonest.[80]

Elliot's analysis has a number of implications for the question at hand. We live in an age of few moral absolutes and, perhaps especially where the legitimacy of what is being considered is something of a grey area, it becomes relevant to consider the attitudes and mores of society at large. A software pirate might well claim that, according to the objective leg of the *Ghosh* test, her actions cannot properly be categorised as dishonest 'according to the ordinary standards of reasonable and honest people'. Both Mirror Group Newspapers and The Yorkshire Post have been caught using pirated software, while in America the New York City Council and, most astonishingly, the United States Department of Justice have been similarly exposed.

Nor should these be considered 'mere' technical infringements of the rules. The United States Department of Justice succeeded in bankrupting a

---

[75] *Textbook of Criminal Law* (1983), G. Williams, pp.727/728; for criticism of Williams' approach see:– *Criminal Law: Text and Materials* (1994), C. Clarkson and H. Keating, p.741.

[76] *R v Ghosh* [1982] 2 ALL ER 689.

[77] *Supra* n.15, para. 2-122.

[78] The Court of Appeal has held on a number of occasions that a *Ghosh* direction will not be necessary in every case and that it depends upon whether the facts of the case point to the defendant's state of mind as being one where a genuine mistake may have been made; see:– *R v Price* (1990) 90 Cr. App. Rep. 409, 411. However, where this direction is given it must be put to the jury in this order; see:– *R v Green* [1992] Crim.LR 292.

[79] *Supra* n.76, 696.

[80] *Supra* n.64, 398.

software company it owed money to, before going on to pirate a further twenty copies of its software, actions which were described by the trial judge as '*trickery, fraud and deceit*'.[81] Finally, it should not be forgotten that even in countries such as Canada, which have a relatively good record on the issue of software piracy, a comparison of the numbers of computers sold to the quantity of software acquired through legitimate channels would appear to indicate that '*two-thirds of the computers must be being used as expensive doorstops*'.[82]

If software piracy is so widespread as to encompass such mainstream, and presumably otherwise honest,[83] organisations then it becomes difficult to see how the actions of any particular individual or organisation can objectively be characterised as dishonest according to the societal leg of the *Ghosh* test. Clearly such a view ignores the extent to which some people might say one thing, whilst doing another – '*Hypocrisy is the homage that vice pays to virtue*', as Francois de La Rochefoucauld famously put it – but then as the objective leg of the *Ghosh* test speaks of 'the *ordinary* standards of reasonable and honest people' (my emphasis), there seems no good reason why a defendant should be judged by a standard which her peers only ever aspire to, rather than achieve to any significant extent.

Furthermore, even where these societal objections can be overcome, the subjective leg of the *Ghosh* test raises additional complications to ascribing the label 'dishonest' to the activities of software pirates. Research has indicated that many of those involved in the non-commercial piracy of software are students[84] who often live in tightly-knit communities – perhaps on university campuses or in colleges. Such individuals live not so much in society at large, but rather in microcosms of society which may have standards which do not exactly mirror the ethical norms of the larger group. If an individual conforms to the standards of the microcosm might he not reasonably claim to have been unaware 'that reasonable and honest people regard what he did as dishonest'? Professor Griew puts it well when he observes that,

> A person reared or moving in an environment in which it is generally regarded as legitimate to take advantage of certain classes of people – perhaps bookmakers or employers – may plausibly claim that he did not

---

[81] Fuller details of this somewhat ignominious day for American justice can be found in *Supra* n.55, pp. 55/56. Inslaw, the bankrupted company, were ultimately quite fortunate as it was only a loophole in the law of bankruptcy which allowed them to sue the Federal government – winning $6.8 million plus legal fees and consequential damages – who would otherwise have been immune from suit.

[82] The Australian (7/11/89), cited in *Supra* n.55, p.53.

[83] As Mirror Group Newspapers were raided by the Federation Against Software Theft during the era of Robert Maxwell I am willing to concede that their inclusion as an example of an honest company is open to question. However, as no less than 80% of their software was found to be pirated – an impressive, if reprehensible, feat by anyone's standards – I felt compelled to mention them in order to highlight the extent of the problem.

[84] See:– Software and the Law', J. Pallette, *PC Week (7/10/86), p.79.*

> realise that his conduct, of which a member of such a class was a victim, was generally regarded as dishonest.[85]

Yet, as Griew continues, 'it is not acceptable that a claim of that sort should be capable of even being advanced.'[86]

11 Is Software Piracy Morally Wrong?

The term 'software theft' is then, plainly, an oxymoron of the first order, but that is not necessarily to say that that should in all circumstances continue to be the case. One of the functions of the criminal law is to apportion blame upon those acts that are morally repugnant to society. Society might have mixed feelings about idealists such as Richard Stallman of the Massachusetts Institute of Technology who argues that,

> '… the full fruits of information technology can be realized only when everyone has the freedom and ability to copy and change programs. …'

Proprietary software obstructs IT progress, he says, and companies should not be allowed to keep their source code secret.[87]

Yet most within society would also recognise that Stallman is exceptionally fortunate to receive funding from sources other than his software – such as GNU-Emacs – which he distributes for free: '*other, more ordinary programmers have to eat*',[88] and it is difficult to believe that there would be many who would condone the organised crime aspect of software piracy which, in any case, all too often involves the commission of other acts which we feel no compunction about criminalizing. The theft of £5.5 million worth of Windows 98 certificates of authenticity in a recent burglary is just one such example,[89] but if it is wrong to take the certificates surely it must also be wrong to take the software? The alternative is to criminalize the theft of the wrapper, but not of the candy, as Doherty observed.[90]

The problem, however, is that attempts to slot the theft of information into the existing order of things are certain to fail. As a society we are still clinging to Nineteenth Century notions of property as we prepare to enter a new millennium. Notwithstanding the concessions that have been made – both by the criminal *and* civil law – in recognising that some intangibles may be owned, the law still does tend to view property in terms of 'things', rather than 'rights'. John Stroud's analysis that 'a system is what a system does',

---

[85] 'Dishonesty: The Objections to Feely and Ghosh', E. Griew *[1985] Crim.LR 341, 353.*
[86] *Ibid.*
[87] *Supra* n.55, p.67.
[88] *Ibid.*
[89] 'Pirates Raid Windows 98 Print Works' , M. Becket, *The Daily Telegraph (27/7/98), p.29.*
[90] *Supra* n.44.

although flawed even by reference to traditional conceptions of property,[91] does tell us quite a lot about how we presently view our possessions. An umbrella is an umbrella because it keeps me dry. A coat may keep me dry too but, as it also provides me with warmth, an umbrella is not a coat. The benefit I derive from my ownership of an umbrella is the benefit of the ability to remain dry. As long as I am not permanently deprived of it then, whilst I may have been inconvenienced by having someone borrow it, it will not have been to such an extent that a criminal sanction is warranted, or in Kantian terms, even demanded.[92] That it will one day rain again is not a matter of conjecture, but rather a somewhat ordinary fact of life, and so the value to me of owning an umbrella remains undiminished.

Yet this account is unsatisfactory in the extreme when we try to apply it to the modern conception of intellectual property rights. It has always required a degree of compromise, as the traditional analysis forces us to ignore the limited malleability which even physical property may possess – borrowing my umbrella for three months may be morally forgivable, borrowing the umbrella which you know I use as a walking stick and without which I am housebound, is likely to be less so. Criminal liability would (probably) still not be imposed upon the umbrella/walking stick borrower, but this is principally because the desire for a rule of general applicability leads us to excuse conduct which, although morally suspect, occurs only infrequently.

However, adopting such an approach towards information forces us to ignore not merely the limited malleability, but rather the *perfect* (or at the very least *near perfect*) malleability which knowledge possesses. A software program that enabled its user to control climatic conditions would have a plethora of potential applications, from the trivial – having the sun shine on me permanently – to the benign – preventing drought and famine in the Third World – to the downright evil – as a weapon of mass destruction. The only limitations on the scope of its use would very likely be the extent of its user's imagination. Yet, whilst we would probably not wish to criminalize the actions of the individual who deprives me temporarily of permanent sunshine, it is less likely in the extreme that we would feel as magnanimous towards the rogue who deprived the Third World of the same program, thus causing drought and famine.

It is all a question of degree. We surely must say that some forms of software piracy should be met with a criminal sanction, but without formulating any offence so widely as to catch lesser conduct which, although very often similar in character, is nevertheless not deserving of quite the same degree of moral obloquy. It is not a satisfactory answer to

---

[91] If Stroud's analysis is taken too literally then it seems that 'a jumbo jet is a bird because it flies': 'It Thinks, Therefore it is … Or is it?', P. Fisher, *The Daily Telegraph Connected Magazine (9/7/98), p.8, p.9.*

[92] See:– A Short History of Western Legal Theory (1992), J. Kelly, p.296.

employ offences such as conspiracy to defraud or abstracting electricity in order to punish those deserving of moral condemnation by skirting around the real issues involved. On what cogent grounds can a conviction or acquittal depend upon such niceties as whether there were two or more persons involved,[93] or whether the amount of electricity used for illicit purposes was measurably different from that which would have been consumed by the computer in its idle state?[94]

Nor is the answer a purpose built solution, as the notion that it is possible to legislate one's way out of a problem in isolation from mainstream law has been shown to be a fallacy on occasions too numerous to even warrant further comment. If the reader doubts the validity of this assertion, I would suggest a re-reading of my earlier criticisms of the *Computer Misuse Act 1990*[95] and a perusal of some of the cases brought under it.[96] Many of those convicted under this provision have been worthy of condemnation, but that should not be allowed to blind us to the wider implications and applications of the *1990 Act*. I stand by my earlier assertion that the possibility – the *likelihood*, even – of executive discretion is no substitute for good, properly thought out, law.

12 Software Piracy: A Continuum Approach

The solution – the only *cogent* solution, at any rate – is to return to the drawing board and to begin again; to ask the question, as does Professor Gretton, '*Do we own things, or rights, or perhaps both?*'.[97] The world has changed almost beyond recognition since our existing conceptions of 'property' and 'ownership' were forged and yet, almost as if in homage to *Bleak House*, we lawyers grind relentlessly on, hitting the same heads against the same brick walls with the same predictable results. We have to accept these changes, rather than attempting to swim against them because:

> If there are no fresh starts in history, if the future is made from fragments of the past, then the discourse of entitlement in an information society will draw on images of information that were produced in a society where information bore a very different relationship to technology, to power, to wealth, a very different relationship even to our own bodies.[98]

---

[93] See:– C. Tapper, *Computer Law* (Longman 1989) pp.285/286; M Wasik, *Crime and the Computer* (1991) pp.115/118.

[94] See:– *R v Siu Tak-Chee* (unreported), cited in *'Computer Misuse'* (1986), Report of the Tasmanian Law Reform Commission.

[95] *Supra* n.31– n.38 and accompanying commentary.

[96] 'Prosecutions Under the Computer Misuse Act 1990', R. Battcock *(1996) 6(6) Computers and Law 22.*

[97] *Supra* n.9.

[98] *Supra* n.1, p.27.

Boyle's contention is that disputes about property rights in information resolve themselves, in part, into disputes about whether the issue "is" in the public or private realm.'[99] This represents, I would suggest, a good place in which to begin considering which sorts of rights we should be protecting, and what particular form that protection ought to take.

Of course there will always be cases such as *Moore v The Regents of the University of California*[100] – in which the question of who 'owned' an individual's DNA fell to be considered – which tax the minds of lawyers and ethicists alike, but then a panacea to cure all ills – attractive though such an approach would be – is simply not practicable in reality. There are both public and private interests in DNA gene sequences, just as there are both public and private interests in a whole range of other forms of information, and the solution will be to ascertain where on the continuum between those two opposites any given interest lies.

Necessarily this involves rejecting – morally and legally – Professor Smith's assertion that the difficulty of deciding such enquiries should lead us to reject this approach altogether,[101] but then it is a fresh approach that is being advocated. In any case, finders of fact are required to make more vexing determinations than this on a regular basis, without anyone seriously suggesting that if a decision is difficult then the conduct that it relates to ought not to be criminalized. That seems to me to be ignoring the fact that whatever else we might expect from a legal system, it is taken for granted that – regardless of their complexity – the courts will determine the issues involved one way or another.

It might seem that re-conceptualising our notions of ownership would involve upheaval that would scarcely be worth the candle, yet to refuse to change is to refuse to acknowledge the extent to which the present state of affairs tends to hamper innovation, rather than foster it. Software programmers are currently afforded either too little protection from the law, which causes them to despair as they see the fruits of their efforts 'stolen' by the unscrupulous. Alternatively, too much protection, whilst protecting the individual programmer concerned, does so by hampering everyone else's ability to compete, often with unforeseen consequences as a result.

A continuum approach between 'public' and 'private', whilst certainly not perfect, would at least allow distinctions to be drawn between the types of interests which are worthy of enhanced (criminal) protection and those which ought not to be protected in any way at all – the examples cited earlier of the Merrill Lynch accounting program and the Hayes modem switch

---

[99] *Ibid*, p.27.

[100] *Moore v The Regents of the University of California*, 793 P. 2d 479 (Cal. 1990), *Cert. denied*, 111 S. Ct. 1388 (1991).

[101] *Supra* n.15 and accompanying commentary.

would seem to represent virtually unarguable instances of the latter,[102] for which even intellectual property protection must surely be regarded as inappropriate.

Certainly such a change would involve upheaval which, given the influence and wealth of some of those with vested interests in this area, might be highly difficult to achieve in practice, but then 'a man's reach should exceed his grasp, or what's a heaven for',[103] and in any case what area of the law is not already in a state of perpetual flux? Furthermore, I would question whether such changes would, in a practical setting, really be so traumatic after all. Over two hundred years ago Kause, commenting on a proposed copyright law, argued cogently and coherently against such a step:

> I can read the contents of a book, learn, abridge, expand, teach, and translate it, write about it, laugh over it, find fault with it, deride it, use it poorly or well – in short, do with it whatever I will. But the one thing that I should be prohibited from doing is copying or reprinting it? . . . A published book is a secret divulged.[104]

His argument was so powerful because he drew upon the full panoply of what had always been his rights in relation to property in order to underline the weaknesses of such a law; but his argument was also fatally flawed because he failed to take account of the extent to which the world had changed whilst his argument had remained static. Just as none of us could now conceive of a world without copyright protection, so it is my belief that future lawyers will look back on us and wonder how we ever made sense of our current interpretation of property.

---

[102] *Supra* n.55 and accompanying commentary.

[103] *Andrea Del Sarto*, Robert Browning.

[104] 'Uber den buchernachdruck', C. Krause *(1783) 1 Deutches Museum 415*, cited in and translated by M. Woodmansee 'The Genius and the Copyright: Economic and Legal Conditions of the Emergence of the 'Author' *(1984) 17 Eighteenth Century Studies 425, 443/444.*