scripted

Volume 8, Issue 1, April 2011

SHOULD THE ENGLISH LEGAL SYSTEM ADOPT THE US LAW OF CYBER-TRESPASS?

Darren Read[*]

Abstract

It has become quite common for old legal rules to be used to regulate new technologies. A key example of this is the resurrection of the rarely used trespass to chattels in the US to cover unauthorised access to computer and networks. However, this judicially constructed law has yet to be exported to other common law jurisdictions. This article considers whether the doctrine of "cyber-trespass" should be copied by the English legal system. Although the law of trespass to chattels is similar both sides of the Atlantic, there are certain underlying differences which are critical in the adoption of cyber-trespass, the most notable being the differences in the need for damage to be proved.

Towards the end of 2008 there was a flurry of cases against Electronic Arts in the US courts over the use of the digital rights management system SecuROM, the first of these cases includes, amongst other things, that the use of SecuROM constitutes cyber-trespass. This goes beyond the previous uses of cyber-trespass as protecting networks from a very direct trespass to a trespass by means of a CD- or DVD-ROM. This newer use of cyber-trespass will be taken as the point of departure with the article using it to illustrate the suitability of cyber-trespass as a legal doctrine in England. To form a considered conclusion other legal avenues for regulating unauthorised computer and network access in England are discussed, most notably Section 3 of the *Computer Misuse Act 1990*.

DOI: 10.2966/scrip.080111.46

[*] Researcher at the Norwegian Research Centre for Computers and Law, University of Oslo.

1. Introduction

Technology generally moves forward faster than the law. This in turn logically leads to problems effectively controlling new technologies so that unwanted behaviour is discouraged. There have been many attempts by the courts in common law countries to apply old laws to these new situations even where it requires a certain amount of judicial creativity to make the old law fit.[1] An obvious example of this process has been the application of an almost forgotten head of action to unauthorised computer access. This is the American lead doctrine of cyber-trespass, expanded from the law on trespass to chattels. It gives computer system owners an action in tort when their systems have been accessed without authorisation and enables them to receive damages for this. However the creation of this law has not been without controversy. The aim of this article will be to discuss whether or not the US law on cyber-trespass should be incorporated into the English system, where it is yet to be developed in the same way. As a necessary part of evaluating the suitability it is important to look at alternative ways that unauthorised access can be governed, for instance using the criminal law, a different action in tort, or possibly creating a new civil offence designed specifically to deal with these situations.

There have been a number of different activities that have lead to the US courts developing cyber-trespass. The original cases dealt with spam and Internet activities such as screen scraping. However, more recently there has been a move to use it as a response to malware and spyware along with the use of restrictive Digital Rights Management Systems that are currently being used by the digital media industry. In this article Digital Rights Management Systems (DRMS) will be taken as a concrete example of where cyber-trespass could come into play. More specifically, the issues surrounding DRMS used to protect computer games will be explored. This will allow real conclusion on the necessity or attractiveness of incorporating cyber-trespass into the body of English law to be drawn.

This article will be based on the laws applicable in England and America and will be split into three parts. Section 1 will give a brief introduction to DRMS to enable the concrete conclusions that are aimed for to be given. Section 2 will look into cyber-trespass. To do this it will first outline the law of trespass to chattels in both England and America before looking in more depth at cyber-trespass itself. This section will conclude by showing that the inherent differences between the US and English law of trespass to chattels are a barrier to cyber-trespass being incorporated satisfactorily into the English system. The final substantive section, Section 3 looks at the most promising alternative to cyber-trespass. That being the criminal provisions contained within the *Computer Misuse Act 1990*. At the end of the article these threads will be drawn together and it will be concluded that none of the options are perfect in their current form. The best option would be a hybrid of the law of cyber-trespass and the provisions of the *Computer Misuse Act*.

---

[1] For example see L Lessig, *Code v.2* (New York: Basic Books, 2006), at 157 for a discussion on the US attempts to re-interpret the Fourth Amendment of the US Constitution when wire tapping became possible.

Trespass to chattels and cyber-trespass, despite the potential importance and continued development of the doctrine, have fallen somewhat out of favour within the academic community. Thus this article has had to rely mainly on analysis of the original founding cases along with the academic writings of the early 2000s. The same is true for the section on the *Computer Misuse Act 1990.* Here the article will rely on the wording of the Act itself with conclusions drawn mainly from analysis of the text, with the scare relevant case law and academic writings supplementing it where possible.

2. DRMS

2.1. Background

Piracy is a real and increasing threat to all forms of digital entertainment media, be it music, films or computer games. However, the actual effect of digital piracy is very hard to ascertain. There have been attempts to quantify the damage to the industries in question, but due to the nature of the beast it is impossible to come up with an exact assessment.[2] To combat this threat the industries have needed to strike a difficult balance between protecting their intellectual creations and not alienating their law abiding customer base. Nowhere is this truer than with customers buying computer games, there have been a number of games which have had disappointing sales figures and customer reviews due to the protection which has been invoked by the publisher.[3]

This article will be concentrate on efforts to protect computer games and their relationship with trespass to chattels. The computer game industry can be split into two sections, console games and PC games. I will be concentrating on the issues surrounding PC games. PC games are more susceptible to unlawful copying due to the inherent open nature of the PC. There are two main approaches that computer game developers have been using to protect their products. They can either opt for software or hardware based Digital Rights Management Systems (DRMS) which protects the computer game software by restricting the actions of the user. The alternative is using an online registration system which can allow a product to be registered and used by a limited number of user accounts which are protected by passwords. Developers can use one or other of these, or a combination of the two.

DRMS are pieces of code which restrict the use of a digital file in conjunction with the rights holders' wishes.[4] They are commonly attached to files protected by

---

[2] The much publicised figures of $250billion monetary losses and 750,000 job losses, which could be found on the US Chamber of Commerce website, have no apparent method in their calculation. In fact no-one seems to know where the numbers actually come from: http://blogs.wsj.com/numbersguy/the-mysterious-provenance-of-piracy-stats-437/ (accessed 28 Mar 2011). The Motion Picture Association of America (MPAA) has had to rectify one of its statistics due to human error; the incorrect figure was 44% of piracy happened on college campuses whereas the "correct" figure was actually 15%. This mistake led to the MPAA lobbying for colleges to filter campus Internet connections http://www.techdirt.com/articles/20080122/18164639.shtml (28 Mar 2011). I will not go further into this as it is beyond the scope of this work.

[3] One of the most notable is *Spore* released by Electronic Arts in Nov 2008. This will be discussed in more detail below.

[4] A more specific definition is impossible. Technology is always moving forwards and the types of protection invoked are continually changing.

intellectual property law to enforce the rights holder's rights. Typical actions that DRMS restrict are copying, burning, and, with digital music files, synchronising to multiple portable devices. However, they can be used to restrict almost any action that the purchaser could do with the file, whether illegal or not. This has lead to some controversy over the role of intellectual property law and how it is enforced.[5]

However, DRMS are not (and probably never will be) 100% secure. This has lead to a kind of arms race between computer game publishers and pirates. Commonly computer games which are protected by a DRMS have their protection cracked and pirated copies are available within weeks; in some case within hours, or even before the game is officially released.[6] Therefore to protect the intellectual property better there have been many moves to strengthen the protection of the DRMS itself. These protections go further than the copyright that the DRMS program would automatically acquire from being a computer programme worthy of copyright protection. In the EU this protection is governed by the Software Directive from 1991.[7] Article 7(1)(c) of the directive provides protection against commercial methods of circumventing DRMS. A similar provision is found in the Digital Millennium Copyright Act in the US.[8] Given the subject of this article a further discussion of anti-circumvention provisions is not necessary.

2.2 SecuROM

SecuROM is a DRMS used by many computer game companies to protect their intellectual property from pirates. It is currently being used by many companies, the most notable being Electronic Arts (EA), Ubisoft, and Codemasters. Some of the most popular games that use the SecuROM system are:

Spore (EA)

The Sims 2 expansion packs (from Bon Voyage and onwards)(EA)

Fifa 09 (EA)

Race Driver Grid (Codemasters)[9]

There is some controversy over how SecuROM works once it has been necessarily installed on a user's computer. Despite the assertions on the official website,[10] some

---

[5] For some examples of these controversies see: A Adams, "Introduction: Valid Protection or Abusive Control?" (2006) 20:3 *International Review of Law, Computers and Technology* 233-237, at 233; L Lessig, see note 1 above, at 179.

[6] For example *The Sims 3* was available two weeks before release: http://www.edge-online.com/news/the-sims-3-leaked-online (accessed 28 Mar 2011).

[7] Directive 91/250/EEC on the legal protection of computer programmes.

[8] 17 U.S.C. §1201.

[9] For a full list of games utilising the SecuROM system see: http://reclaimyourgame.com/index.php?option=com_content&view=article&id=45&Itemid=11 (accessed 28 Mar 2011) – please note, that at the time of submission the "Reclaim Your Game" website was undergoing a migration to a new server and was unavailable. Because of that I cannot guarantee that any of the "Reclaim Your Game" links will work when the migration has been completed.

contend that the software is a form of rootkit which affects the inner workings of the computer. This is reminiscent of the Sony Rootkit scandal which culminated in 2005 where Sony BMG included a copy protection system on its audio CDs to protect their intellectual property when the CDs were used on a PC.[11] It was discovered by Mark Russinovich[12] that the system Sony used had many similarities to spyware[13] and was effectively uninstallable without risking further damage to the computer system. The legal ramifications were never fully ascertained as Sony BMG settled the case by providing replacement CDs for all users who purchased infected products.[14] They have also released a programme for uninstalling the DRMS.[15]

Whether or not the system is a rootkit and whether or not it can affect the inner workings of the user's computer is up for debate. But what is certain is that, in most cases, the SecuROM software, a standalone piece of software which is installed onto the user's computer when a game is installed, is put there without the user's permission, and it is this that provides the basis for a claim in cyber-trespass.[16] When the owner of a system removes a game from their system which uses SecuROM the SecuROM programme itself will not be removed. In fact there is no easy way of removing the application from the system. Either the user must download another programme to remove SecuROM or follow a long and complex process which, if done incorrectly, could damage his or her system.[17]

The use of SecuROM has lead to a number of court cases. The most notable, and first was against Electronic Arts (EA) over their use of SecuROM in protecting their game "Spore". This was released on 4 September 2008,[18] and at this point users were restricted to three installations of the game. This was increased to five installations after a number of complaints.[19] Installations could be recovered by contacting EA and pleading your case to be allowed another. Now it is possible to do this online.[20] There

---

[10] https://support.securom.com/faq.html (accessed 28 Mar 2011).

[11] B Scheier, "Real Story of the Rogue Rootkit" (2005) available at www.wired.com/politics/security/commentary/securitymatters/2005/11/69601 (accessed 28 Mar 2011).

[12] His research was published in a blog entry which can be found at http://blogs.technet.com/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx (accessed 28 Mar 2011).

[13] The *Encyclopædia Britannica* defines spyware as a: "type of computer program that is secretly installed on a person's computer in order to divulge the owner's private information, including lists of World Wide Web sites visited and passwords and credit-card numbers input, via the Internet." Available at "Spyware." 2009. *Encyclopædia Britannica Online*. 3 Sept 2009.

[14] Information of the settlement can be found at http://www.eff.org/cases/sony-bmg-litigation-info (accessed 28 Mar 2011).

[15] Available at http://cp.sonybmg.com/xcp/english/updates.html (accessed 28 Mar 2011).

[16] This will be discussed fully in the next section.

[17] Process available here: http://reclaimyourgame.com/index.php?option=com_content&view=article&id=68&Itemid=40 (accessed 28 Mar 2011).

[18] http://eu.spore.com/whatisspore/platforms.cfm (accessed 28 Mar 2011).

[19] A new installation could be triggered by a number of actions, such as upgrading hardware components of the computer or installing a new operating system. This is not simply installing on a new machine.

[20] http://eu.spore.com/whatisspore/article.cfm?id=32381 (accessed 28 Mar 2011).

was wide disappointment over the eventual product that was released, mainly due to the use of SecuROM. For example users only gave it 4.6 out of 10 on the *Metacritic* review website, compared with 84 out of 100 for professional critic reviews.[21] The difference between critic ratings and user ratings shows that the use of a draconian DRMS is unpopular with computer users and may show evidence that the use of them can affect consumer preferences.

On 22 September 2008, only two weeks after the release of the game, Melissa Thomas filed a law suit against EA for the use of the SecuROM system on a number of grounds. This law suit was voluntarily dismissed by the plaintiff so that it can be consolidated with a number of other cases which have been filed against EA for the same reasons. The crux of the cases is the inclusion of the SecuROM system as a "separately installed, stand alone, uninstallable DRM program" and that this programme is not disclosed anywhere in the literature which accompanies the game, either in the instruction manual or the End User License Agreement (EULA). In the pleadings for the case there was a list of fifteen legal questions. The most pertinent was: "M: Whether by its conduct, defendant has trespassed on the computers of all persons who installed the Spore computer game".

The first seven questions all deal with the same legal issue, namely disclosure and authorisation. These are important aspects of most computer crimes, especially those which will be dealt with here. Question M looks at trespass to chattels which will be the main discussion of this article.

Along with the pleadings in the lawsuit there have been many reports of the SecuROM system effecting users' computers in ways that are far from desirable.[22] These remain, however, just reports. It is notoriously difficult to ascertain the direct cause of a problem with a computer system. These problems could have been caused by SecuROM on its own, SecuROM conflicting with another piece of software found on some computers, or could be a coincidence in timing. What is not debatable is the necessary feature of such systems to be running in the background whenever the computer is functioning. It is always working to make sure that the user is not doing anything that the rights holder does not want them to do with their programme. This inevitably uses computer processing power which will affect the computer's performance. If a computer is using part of its processing power to do one thing then it cannot use that power to perform other functions that the user may ask it to do, therefore slowing the computer down. The extent will depend on the power which the computer has, if it has a large processing capacity then the effect will be negligible, however, with older, less powerful machines the effect will be far greater.

3. Trespass to Chattels

[21] http://www.metacritic.com/games/platforms/pc/spore?q=spore (accessed 28 Mar 2011). Figures correct as of 21 Mar 2011, although user score subject to change as more reviews are added.

[22] For a list of different problems that have stemmed from the installation of SecuROM visit http://reclaimyourgame.com/index.php?option=com_content&view=article&id=52&Itemid=13 (accessed 28 Mar 2011). Problems that have been experienced include: disablement of CD/DVD drives; wrongly identifying legal software as emulation software and then disabling it; or interfering with the users Internet firewall.

Trespass to chattels is a very old area of common law that has experienced something of a renaissance in the US. However, the renewed interest in this area has not taken off in other common law countries yet.[23] This section will be split into three main parts. The first part will look at the law of trespass to chattels in both England and America; this analysis will highlight the differences between the two. Secondly it will look at how this almost forgotten law has been reincarnated to deal with computers in America, discussing whether this has been a good thing or not. Finally it will discuss whether or not it would be appropriate for the English courts to follow the American example and stretch trespass to chattels to include computer related claims. To do this the SecuROM example will be used to give it some grounding in a real situation.

3.1. The State of the Law

3.1.1. English Law

Trespass to chattels (or trespass to goods)[24] is scarcely used in the English legal system.[25] Therefore there is some ambiguity over the definition of the law and what is needed to succeed in a claim. However what is certain is that a trespass is "[a] wrongful direct interference with another person or with his possession of land or goods... a direct and immediate interference with person or property, such as striking a person, entering his land, or taking away his goods without his consent".[26] So trespass to chattels is an immediate and direct interference with property.

What is not clear, however, is whether it is actionable per se or if there is a need for damage to be proved. Even in the leading works on tort law there is disagreement over this requirement. For example in *Salmond & Heuston on the Law of Torts* they say that "a trespass to goods is actionable per se without any proof of actual damage. Any unauthorized touching . . . is actionable at the suit of the possessor of it, even though no harm ensues".[27] In the case of *Leitch v Leydon*[28] Lord Blanesburgh stated that: "The wrong to the appellants in relation to that trespass is constituted whether or

---

[23] Following extensive case and literature searches I feel safe in my conclusion that this is the case. I have not been able to find any mention of trespass to chattels being used in such a way anywhere but the US. This is also backed up by M W S Wong, "Cyber-trespass and 'Unauthorised Access' as Legal Mechanisms of Access Control: Lessons from the US Experience" (2007) 15:1 *International Journal of Law and Information Technology* 90-128 at 91.

[24] The terms "trespass to chattels", "trespass to goods", and "trespass to property" seem to be interchangeable with trespass to chattels seemingly the favoured term in the US and trespass to goods the favoured term in England. This will generally use the term trespass to chattels as this is the term generally used in conjunction with cyber-trespass as it is of American origin.

[25] Following a simple case search on a law database it came up with forty one reported cases dealing with trespass to goods. In most of these cases trespass to chattels was merely an incidental element and not much discussed. The main issues in the cases were anything from Landlord and Tenant to criminal and civil evidence and procedures.

[26] "Trespass n." in J Law and EA Martin, *A Dictionary of Law* (Oxford: OUP, 2009) available at http://www.oxfordreference.com/views/ENTRY.html?subview=Main&entry=t49.e4041 (accessed 28 Mar 2011).

[27] R Heuston and R Buckley, *Salmond & Heuston on the Law of Torts*, 21st ed (London: Sweet & Maxwell, 1996), at 95.

[28] *Leitch v Leydon* [1931] AC 90.

not actual damage has resulted therefrom either to the chattel or to themselves".[29] However this is only *dicta* as trespass formed no part of the final judgement and the discussion on English law was not applicable to this Scottish case. The Oxford *Dictionary of Law* also defines trespass as being actionable per se.[30] On the other hand, others, such as Markesinis and Deakin, are less clear over the lack of a damage requirement and hold that damage may be required depending on the facts of the case: "It is not altogether clear whether liability is based on damage or whether the tort is actionable *per se*. It may be possible to distinguish between deliberate touchings, which are actionable per se, and unintended or careless acts of touching, which require damage".[31] Despite the uncertainty, it can be suggested that it would not be incorrect to assume that trespass to chattels is actionable per se and that damage is not required. All three forms of trespass: land; chattels; and the person come from the same legal ancestry and there is no evidence that the courts have restricted the applicability of trespass to chattels only to cases where there has been some damage.

3.1.2. US Law

A good summary of the law on trespass to chattels in America can be found in the *Restatement (second) of torts 1965*, s 217. This states:

> A trespass to a chattel may be committed by intentionally
>
> (a) dispossessing another of the chattel, or
>
> (b) using or intermeddling with a chattel in the possession of another.[32]
>
> Where intermeddling means "intentionally bringing about a physical contact with the chattel". However trespass to chattels is only actionable where there has been some "damage" as defined by section 218 of the restatement:
>
> One who commits a trespass to a chattel is subject to liability to the possessor of the chattel if, but only if,
>
> (a) he dispossesses the other of the chattel, or
>
> (b) the chattel is impaired as to its condition, quality, or value, or
>
> (c) the possessor is deprived of the use of the chattel for a substantial time, or
>
> (d) bodily harm is caused to the possessor, or harm is caused to some person or thing in which the possessor has a legally protected interest.

---

[29] *Leitch v Leydon* per Blanesburgh LJ, at 106.

[30] "Trespass is actionable per se, i.e. the act of trespass is itself a tort and it is not necessary to prove that it has caused actual damage." J Law and E A Martin, see note 26 above.

[31] S Deakin et al, *Markesinis & Deakin's Tort Law*, 6th ed (Oxford: OUP, 2007), at 484.

[32] *Restatement (second) of Torts 1965* s.217.

When compared to the English law, the damage requirement is a striking, and considerable difference. It is this that plays a major role in assessing cyber-trespass' suitability for English law.

3.2 Cyber-trespass

It was in relation to telecommunications that trespass to chattels was first used to deal with technological issues. In *Thrifty Tel v Bezeneck*[33] the defendants were held to be liable under trespass[34] after hacking into Thrifty's long distance telephone network. It is this case that lays down the foundations for all other further uses of the law to deal with networks and computer systems. There were significant hurdles which had to be jumped before a claim could work. Firstly, what property is being trespassed upon, and how this has been subject to physical contact. Secondly, there is the need under US law for damage to be apparent before it is actionable (section 218), this could prove difficult when it comes to electronic technology and depends on how broadly damage is to be interpreted.

The courts in *Thrifty* decided that the chattel that was being trespassed upon was the phone network. The problem then was the physical contact. There was no physical contact by the defendants to the network. They did not go to an old fashioned telephone exchange and start moving wires around themselves; they were doing it from afar trying to hack the system by "phreaking". The courts decided that the electronic signals that the plaintiffs were creating and "touching" Thrifty's network with were "sufficiently tangible to support a trespass cause of action". In this case the idea of damage was given only a cursory mention, but was held to be apparent from the facts.

The Thrifty case was followed by the Ohio courts in the first computer network related case. This was as a response to spam and was before the *US CAN-SPAM Act 2003* came into force which provides custom built legal protection against spam. In *Compuserve v Cyber Promotions*[35] Compuserve sued Cyber Promotions for damages after they had sent a multitude of spam emails to Compuserve customers. The court followed the reasoning in *Thrifty* with regards to the physical contact that trespass necessitates, electronic signals are enough to constitute such a touching. The damage here was, controversially, not wholly reserved to the computer system. The court decided that a number of consequences could constitute damage. Firstly the extra burden that was being placed on Compuserve's system, this used up network space, processing power, and memory. This finding was based on s 218(b) of the restatement, that the chattel (the computer system) had been impaired as to its "condition, quality, or value". It was held that the claimant need not show that the physical condition of the chattel was impaired, but merely the value of it as a whole.[36] However, more controversially, it was also held that the plaintiffs could claim for the loss of working hours trying to block the unwanted spam, along with any other costs

---

[33] *Thrifty Tel v Bezeneck* 54 Cal. Rptr. 2d 468 (Cal. Ct. App. 1996).

[34] Incidentally Thrifty was originally trying to prove conversion, but it was the courts that substituted the conversion claim for one of trespass to chattels.

[35] *Compuserve v Cyber Promotions* 962 F. Supp. 1015 (S.D. Ohio 1997).

[36] *Compuserve v Cyber Promotions*, per Graham, District Judge at 1021-1022.

involved in that protection. The loss of customer goodwill was also "damage" as per the restatement. These last aspects of the decision were questionable as their proximity to the trespass claim is remote. The whole reasoning behind damage has been criticised by many in the academic world, especially Dan Burk in his article "The Problem with Trespass"[37]

> If such examples as I have suggested begin to sound a bit silly, that should perhaps indicate the degree of regard properly paid to the "trespass" of electrons upon computers intentionally connected to a network known to carry such electrons. The Restatement test guards against such trivial contacts by requiring that the contact rise to the level of some substantial interference equivalent to physical seizure of the chattel or similar deprivation of its use. This may occur if the chattel is damaged or impaired as to its condition, quality or value. But in the case of Cyber Promotion's "impinging electrons"...the physical contact with the equipment is of course too slight to constitute seizure or deprivation, or cause damage.[38]

There has been a significant number of similar cases going through the courts in America since the Compuserve decision. The most notable being *eBay v Bidders Edge*,[39] a number of cases which involve America Online (AOL)[40] and *Register.com, Inc v Verio, Inc*.[41] All of which have had to decide what constitutes damage, with some controversial outcomes.[42] But it is clear that the policy reasons for finding trespass to chattels in these claims are persuasive. In the eBay case Bidders Edge was using a web spider to crawl through the eBay auction site to create its own service based on, amongst others', eBay's auctions. They had tried to negotiate a license with eBay, but this was refused and Bidders Edge went on to crawl eBay's site regardless.[43] Here it was clear that the courts wanted to dissuade other "free-riders" from making money out of someone else's work.[44] In *Register.com* the plaintiff was trying to stop the defendant (Verio) from using its WHOIS database without permission by sending a large number of emails requesting information. This was after they had tried to negotiate a license to use the database but had been rejected.

---

[37] D Burk, "The Trouble with Trespass" (1998) 3 *Journal of Small & Emerging Business Law* 27.

[38] Ibid at 9-10. He goes on to suggest that following the logic to its conclusion there could be cause for the creation of the law of "trespass to toasters" insofar as they can be (really) damaged by a surge of electrons through the power grid. Here there would be touching of property by flowing electrons (following Compuserve and Thrifty) regardless of the fact that that is the purpose of the grid and the toaster.

[39] *eBay v Bidders Edge* 100 F. Supp. 2d 1058 (N.D. Cal. 2000).

[40] *America Online, Inc. v IMS*, 24 F.Supp.2d 548 (E.D.Va.1998); *America Online, Inc. v LCGM, Inc*., 46 F.Supp.2d 444 (E.D.Va.1998); *America Online, Inc. v Prime Data Systems, Inc.*, 1998 WL 34016692 (E.D.Va. Nov 20, 1998).

[41] *Register.com, inc. v Verio, inc.* 126 F. Supp. 2d 238 (S.D.N.Y. 2000).

[42] See, e.g., L Quilter, "The Continuing Expansion of Cyberspace Trespass to Chattels" (2002) 17 *Berkeley Technology Law Journal* 421.

[43] For a full discussion of the Bidders Edge case and an analysis of the balancing act between primary and secondary aggregators on the Internet see R Warner, "Border Disputes: Trespass to Chattels on the Internet" (2002) 47 *Villanova Law Review* 117.

[44] How this decision would affect the myriad of price comparison sites is up for discussion here.

The AOL cases dealt with spam (again before the *CAN-SPAM Act*) and again there is good policy reason to find in favour of the plaintiff. All of these cases effectively came to the just conclusion for the case, but have left a somewhat controversial and patchy set of precedents.

The final case in the creation of cyber-trespass is *Intel v Hamidi*.[45] This case involved a disgruntled ex-employee (Hamidi) of Intel who, after leaving the company, started a campaign against them. He would send current employees emails telling them how he had been treated by Intel. In the first instance the court followed the previous cases on point and decided this was trespass. Although Intel was not a service provider as such, so the emails on the system could not affect customer goodwill, the time taken by the employees to sift through Hamidi's (not too frequent) emails was held to be enough to constitute damage. Staff also took some time trying to block Hamidi's emails. This along with the inevitable using of computer memory and processing cycles was held by the courts to amount to damage. Unlike the previous cases, the Hamidi case lacked the clear policy reason for a finding of cyber-trespass. The emails were not anywhere near the quantities of the other Spam cases.[46] There were no unfair business practices, no loss of reputation, and no real additional strain on Intel's system. The fairly small volume of emails was of no real consequence to the memory or processing abilities of Intel's network. On appeal the California Supreme Court went some way to restricting the applicability of trespass to chattels to the digital networked environment. The court gave very succinct summary of the judgement which is worth quoting in full:

> After reviewing the decisions analyzing unauthorized electronic contact with computer systems as potential trespasses to chattels, we conclude that under California law the tort does not encompass, and should not be extended to encompass, an electronic communication that neither damages the recipient computer system nor impairs its functioning. Such an electronic communication does not constitute an actionable trespass to personal property, i.e., the computer system, because it does not interfere with the possessor's use or possession of, or any other legally protected interest in, the personal property itself... The consequential economic damage Intel claims to have suffered, i.e., loss of productivity caused by employees reading and reacting to Hamidi's messages and company efforts to block the messages, is not an injury to the company's interest in its computers—which worked as intended and were unharmed by the communications—any more than the personal distress caused by reading an unpleasant letter would be an injury to the recipient's mailbox, or the loss of privacy caused by an intrusive telephone call would be an injury to the recipient's telephone equipment.[47]

This decision has attempted to reign in the scope of cyber-trespass in the US courts. Although, not a binding precedent in the other states, it is a persuasive argument and arguably the correct interpretation of the law. Only damage to the computer system

---

[45] *Intel Corp. v Hamidi* First decision: 114 Cal. Rptr. 2d 244 (2002), reversed by: 30 Cal. 4th 1342 (2003).

[46] There were six mail shots over a period of two years. *Intel v Hamidi* per Werdegar, J, at 1346.

[47] *Intel v Hamidi* per Werdegar, J. at 1347.

itself can lead to an action in trespass. As Burk puts it "employees are not chattels".[48] Further it would appear that any use of memory or processing cycles must actually cause some impairment to the system. If it is merely negligible (as was the case with Intel's system) then it cannot amount to a trespass.

All of the above cases have dealt with email or screen scraping. The situation that is being concentrated on here is slightly different. The situation involving SecuROM and other similar DRMS involve the secret installation of software. This type of complaint has been the subject of some later cases; most notably *Sotelo v DirectRevenue, LLC*.[49] This case involved the secret bundling and installation of spyware[50] with legitimately downloaded software. This was the first case to involve a private user's computer rather than a large network system. The Illinois court decided that this was irrelevant to the claim. Further, the court used the Compuserve reasoning when it came to deciding what constitutes damage.[51] So using Internet connection, processing cycles, and memory is enough to impair the system. Putting this together with the court's reasoning behind ignoring Intel as persuasive it would appear that the test for damage is thus: The damage caused must be to the computer system, not to other incidental objects (employees). It must also be real and noticeable, not so insignificant to make no difference to the performance of the system in question. But most importantly it held that the secret bundling of spyware onto a private user's computer can amount to a trespass (as long as there is damage). This is directly analogous to the example I have used with computer game DRMS and SecuROM in particular. However, once more, there are strong policy reasons behind this decision. Spyware is bad and any means to help in the fight against it is welcome. But this cannot be said about DRMS. They are not programmes which are there to spy on people and help direct advertising (or worse). They are there to protect the intellectual property of the rights holder. There have to be questions over whether the court would have agreed with the plaintiffs in the Sotelo case if it was a DRMS rather than spyware.

Another potential problem with using cyber-trespass for the DRMS situation is the lack of a physical connection between the two parties. The reasoning behind allowing cyber-trespass in America is that the flow of electrons is enough to count as physically touching the chattel. This already stretched definition of touching could need to be stretched even further when the software complained of is stored on a disc rather than coming directly over the network. There is no "physical" connection for the electronic signals to travel down between the two systems. This leads to the question over whether trespass to chattels can be indirect. Whether putting a program on a disc and then the user installing the contents of that disc onto their computer can

---

[48] D Burk, see note 38 above, at 11.

[49] *Sotelo v DirectRevenue, LLC* 384 F.Supp.2d 1219 (N.D.Ill. 2005). See also *Thomas Kerrins v Intermix Media, Inc.* No. 2: 05-cv-05408-RGK-SS (C.D. Cal. Jan. 10, 2006). Both of these cases were preliminary hearings where the courts dismissed the defendants' claims to dismiss. There have been no final rulings at the time of writing.

[50] In his article Mathias Klang gives a good four point definition of spyware. M Klang "Spyware: Paying for Software with our Privacy" (2003) 17:3 *International Review of Law, Computers and Technology* 313-322 at 314.

[51] It dismissed the relevance of *Intel v Hamidi* on the basis that there was no measurable impairment of Intel's system.

amount to a trespass within the wording of the law. The actual software that is being placed on the computer is directly analogous to the spyware example from Sotelo, but the method of administering the programme is not. The US law in the Restatement of Torts explicitly says that the trespass can be indirect, for example throwing an object deliberately to damage the chattel.[52] This would suggest that an indirect physical intermeddling such as using a disc would fit within this definition.

3.3. Incorporation into English Law?

As has been discussed above trespass to goods in English law is likely to be actionable per se. This is not the case in American law. Originally the damage requirement for cyber-trespass was interpreted very widely to include any use of a computer system whether there was actually an impairment. It could also include loss of employee time and goodwill of customers. This has been severely reined in by *Hamidi* to require actual damage or impairment to the computer system only. This will restrict the scope of cyber-trespass considerably. If the previous cyber-trespass cases followed *Hamidi* it is doubtful that they would all have succeeded. For instance Bidders Edge's crawling and screen scraping of eBay was not having a real detrimental effect to eBay's computer system. Register.com's system was not being impaired by Verio's WHOIS requests; the system was designed to be searched in that way. Staff time was being used up, but this should not count towards damage for trespass. The spam cases are the only ones which are likely to have succeeded as spam can have a real detrimental effect on a computer system's usability. However, in America at least, trespass to chattels is unlikely to be used for these cases since the inception of the *CAN-SPAM Act*.

Without the damage requirement in English law cyber-trespass would overreach. The number of situations where it would be applicable would be too numerous to be practical. For instance search engine bots crawling over websites, categorising them for future searches. These cause no harm, but arguably there is a trespass. The same goes for price comparison sites. To stop trespass to chattels overreaching and causing a lot of harmless activities becoming unlawful the damage requirement is needed to limit the scope of the law. English law would need to find some other limiting factor to keep cyber-trespass under control if it were to follow the US example. For this reason it appears that cyber-trespass would be an unwelcome addition to English law.

Where the American law allows for an indirect touching, it would appear that this is not the case in England. The definition in the Oxford *Dictionary of Law* calls for a "wrongful direct interference with...goods".[53] But to what does "direct" refer? Does the interference (the "unauthorized touching") have to be direct in that the physical contact has to be direct? In which case trespass to chattels would struggle to apply to DRMS situations in English law where there is no direct touching by electrons. Or does it simply mean that the impairment has to be direct, in which case the state of the law is similar in this regard to the American law and cyber-trespass would still be possible in cases where discs are involved. As there is no case law on point, it is unclear which way the English courts would go, but, for cyber-trespass at least, the latter interpretation would be preferable.

---

[52] *Comment e. of Restatement (second) of Torts* s 217.

[53] J Law and E A Martin see note 26, above.

Overall, although the law on cyber-trespass since the Intel decision is a good and practical way of governing the problems which have come up regarding unauthorised network access, it would be unsuitable for incorporation into the English system. The damage requirement is required to reign in cyber-trespass' scope, without it would be too broad a law.

4. The *Computer Misuse Act 1990*

Originally criminal damage was applicable to any damage caused to a computer, be it physical damage or damage to the workings of the computer. Criminal damage is set out in section 1 of the *Criminal Damage Act 1971*:

> A person who without lawful excuse destroys or damages any property belonging to another intending to destroy or damage any such property or being reckless as to whether any such property would be destroyed or damaged shall be guilty of an offence.

S 10 of the act sets out what is to be considered as property with regards to criminal damage. Unlike with theft,[54] property is restricted to tangible property, be it real or personal,[55] so it can be land but not something intangible or a "thing in action". The cases of *Cox v Riley*[56] and *R v Whiteley*[57] made it clear that this did not mean damage to computer data was outside of the scope of the act. Rather, that the damage itself didn't have to be tangible as long as the property that was damaged was tangible. So in terms of criminal damage and computer data the damage is done to the physical object, the computer, by damaging the intangible aspect of it, the data held on the computer. However this was all made immaterial by s 3(6) of the *Computer Misuse Act 1990* which specifies that:

For the purposes of the [1971 c. 48.] *Criminal Damage Act 1971* a modification of the contents of a computer shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition.

This provision has now been moved to s 10 of the *Criminal Damage Act* following the *Police and Justice Act 2006*, sch 14.

The *Computer Misuse Act 1990* was created to provide protection for computers and computer networks from hackers and other computer crime, an increasing problem at a time when computing was beginning to take off. There are two main crimes which are covered by the act; unauthorised access to a computer system[58] and unauthorised modification of computer material.[59] There is also a third offence which is unauthorised access with intent to commit a further offence, in essence an aggravated

---

[54] *Theft Act 1969*, s 4.

[55] *Criminal Damage Act 1971*, s 10.

[56] *Cox v Riley* (1986) 83 Cr. App. R. 54.

[57] *R v Whiteley (Nicholas Alan)* (1991) 93 Cr. App. R. 25.

[58] *Computer Misuse Act*, s 1.

[59] *Computer Misuse Act*, s 3. This has now been replaced by section 36 of the Police and Justice Act 2006, which has created the offence of unauthorised acts with intent to impair operation of computer, etc. I will discuss this amendment below.

form of the s 1 offence.[60] Each offence will be looked at in turn, starting with a brief look at s 1 and then a more detailed look at the s 3 offence. It will be concluded that the *Computer Misuse Act*, through its s 3 offence, should be amended to include tortuous liability in addition to its current criminal liability. That the *Computer Misuse Act* only deals with criminal liability is its major weakness as an alternative to cyber-trespass.

4.1. Computer Misuse Act s 1

Many programmes "phone home" to their creators with information about the system on which they are being run. This can be used by the company in a multitude of ways, for instance to research on what systems people are using their programmes on, or, in the case of many DRMS to help in the fight against piracy. For instance the SecuROM system can be set up to "phone home" and includes in these "calls" certain pieces of potentially personal data such as IP address and other facts about the system that it is being run on, such as the operating system.[61]

S 1 of the *Computer Misuse Act* governs unauthorised access to a computer system. This has also been amended by the *Police and Justice Act 2006*, s 35. I have set the provision out below [with the 2006 amendments]:

> (1) 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 [or to enable any such access to be secured];
>
> (b) the access he intends to secure [or enable to be secured] is unauthorised; and
>
> (c) he knows at the time when he causes the computer to perform the function that that is the case.
>
> (2) The intent a person has to have to commit an offence under this section need not be directed at—
>
> (a) any particular program or data;
>
> (b) a program or data of any particular kind; or
>
> (c) a program or data held in any particular computer.

The purpose behind this provision is to protect computer systems from hacking. It is worded in such a way to cover access without any further actions.[62] It protects against

---

[60] *Computer Misuse Act*, s 2.

[61] F Jennings and J Yates have applied the s 1 offence to screen scraping, such as was the case in Bidders Edge. They suggest that screen scraping can satisfy the offence where there is knowledge that the scraping is unauthorised. However, they contend that the main problem lies with either persuading the CPS of the merits of the case or having to finance a private prosecution. F Jennings and J Yates, "Scrapping Over Data: Are the Screen Scrapers' Days Numbered?" (2009) 4:2 *Journal of Intellectual Property Law & Practice* 120 at 127-8. Bringing about a prosecution is also a significant problem when it comes to applying the s 3 offence to the DRMS case, as will be discussed below.

[62] This is covered by s 2 of the act; unauthorised access with intent to commit or facilitate commission of further offences.

any unauthorised access to computer data which means it can potentially be used with reference to perfectly legitimate computer programmes phoning home with data. It is clear that there is access to data held on the computer, for instance details on the operating system and the computer's IP address. The next thing that would need to be proved was that the access was unauthorised. If there was included in the license agreement pertaining to the programme a clause which sets out that the programme is likely to phone home and with what information then there would be authorisation and there would be no offence. An example would be section 4 of the "Spore End User Licensing Agreement" ("EULA") which states that:

> *4. Consent to Use of Data***.** To facilitate technical protection measures, the provision of software updates and any dynamically served content, and product support and other services to you, including online play, you agree that EA and its affiliates may collect, use, store and transmit technical and related information that identifies your computer (including an Internet Protocol Address and hardware identification), operating system and application software and peripheral hardware. EA and its affiliates may also use this information in the aggregate, in a form which does not personally identify you, to improve our products and services and we may share anonymous aggregate data with our third party service providers.

4.2 Computer Misuse Act s 3, as amended by the Police and Justice Act 2006

The original s 3 of the *Computer Misuse Ac*t was replaced in the *Police and Justice Act* to protect computer systems from denial of service attacks. These are attacks which overload a system with data so it can no longer function properly. There was disagreement over whether these would fall under the old s 3. In fact in the case of *DPP v Lennon*[63] the court of first instance decided that a denial of service attack perpetrated by sending millions of emails was not contrary to s 3. The (somewhat flawed) logic behind the decision was that since the company that was attacked had an email server which was designed and installed to deal with incoming and outgoing emails then it was not an unauthorised act to send the company emails. To extend this authorisation to purposefully sending millions of emails with the intent to disable the network would seem absurd. The case was later appealed and sent back to the courts to be reheard, but the confusion over the status of denial of service attacks was enough to encourage the government to review the law.[64]

S 3 now outlines the offence of "unauthorised acts with the intent to impair, or with recklessness to impairing, operation of a computer, etc." The full text of the section is as follows:

> (1) A person is guilty of an offence if—
>
> (a) he does any unauthorised act in relation to a computer;

---

[63] *DPP v Lennon* [2006] EWHC 1201 (Admin).

[64] See e.g. I Walden, *Computer Crimes and Criminal Investigation* (Oxford: OUP, 2007), at 172-178. Walden contends that it is that "an 'act' is now explicitly defined as a 'series of acts' which enables [denial of service] traffic to be treated as a sum rather than as individual messages" that makes s 3 applicable to denial of service attacks.

> (b) at the time when he does the act he knows that it is unauthorised; and
>
> (c) either subsection (2) or subsection (3) below applies.
>
> (2) This subsection applies if the person intends by doing the act—
>
> (a) to impair the operation of any computer;
>
> (b) to prevent or hinder access to any program or data held in any computer;
>
> (c) to impair the operation of any such program or the reliability of any such data; or
>
> (d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done.
>
> (3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (d) of subsection (2) above.
>
> (4) The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to—
>
> (a) any particular computer;
>
> (b) any particular program or data; or
>
> (c) a program or data of any particular kind.

The questions that have to be asked are, firstly was there an unauthorised act to the computer system (s (1)(a)). The second aspect that would need to be proved is that there was intention or recklessness and knowledge on behalf of the accused.

4.2.1. Actus Reus

"Act" is not further defined in the Act and there is no case law on point yet. However, it is clearly meant as a very broad offence and should mean basically anything done in relation to a computer. This broad scope of "act" is restricted by the rest of the section. Authorisation is dealt with under s 17 of the act, more specifically s 17(8):

> (8) An act done in relation to a computer is unauthorised if the person doing the act (or causing it to be done)—
>
> (a) is not himself a person who has responsibility for the computer and is entitled to determine whether the act may be done; and
>
> (b) does not have consent to the act from any such person.

As Neil MacEwan puts it: "If the accused was not entitled to control the [act] in question, and did not have the consent of someone who was, the requisite lack of

authority is established".[65] This is a simple test of authority that would exist in any realm of life, be it electronic or with regards to real property.[66]

So any change to a computer without consent would fit under this provision. In the case with the SecuROM software, there was no disclosure that the program was a separate third party piece of software so there could be no consent from the users of the computers that became "infected" by the software. There could be an argument over implied consent, giving that there is notice of a DRMS being used by the Spore game, therefore the user has consented to such a DRMS being utilised. But since there is no notice telling the user that it is not actually part of the game which is being installed, but a stand-alone program which installs itself at the very heart of the system, then this line of argument would, and should, ultimately fail. Here it is useful to use the analogy from the comment on *DPP v Bignall*: "If I give you permission to enter my study for the purpose of reading my books, your entering to drink my sherry would surely be an unauthorised 'access' to the room as well as to the sherry".[67] The user may give authorisation for the use of DRMS to protect a company's intellectual property, but it does not follow that this authorisation is for the installation of a stand-alone programme which is placed at the heart of the computer system and cannot be (easily) uninstalled even if the game is uninstalled.

There are also some problems when it comes to defining impairment. Does it require some catastrophic system failure or a small drop in performance? Or more likely somewhere in between? Judicial thoughts on this matter have been lacking from the body of case law on this subject. Following the rule in cyber-trespass it would appear that the using up some of the processing power of a computer is sufficient if the effect is noticeable. Since the *Computer Misuse Act* sets down criminal liability it is not unreasonable to expect there to be a higher threshold than in tort law.[68] There are already such principles enshrined in the law of criminal damage. The damage caused for criminal damage to be found must be more than *de minimus*; that is more than negligible. In *Morphitis v Salmon*[69] for example a scratch on a scaffolding pole was held not to constitute criminal damage as it did not affect the usefulness of property. If such a principle were to be used for deciding the impairment threshold then the impairment should have to go further than merely being noticeable, but be significant. In the case of using processing power this should have a significant effect on the performance of the computer. In the SecuROM example, the effect of the DRMS

---

[65] N MacEwan "The Computer Misuse Act 1990: Lessons from its Past and Predictions for its Future" (2008) 12 *Criminal Law Review* 955-967 at 957.

[66] For an in depth discussion of the meaning of authorisation see e.g. O Kerr, "Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes" (2003) 78:5 *New York University Law Review* 1596-1668.

[67] *DPP v Bignall* [1998] 1 Cr. App. R. 1.

[68] Downing uses the analogy of an employee playing multi-player online games over the company's network connection against the express rules of the company. "Although such an activity might slow down the network slightly, it would be inappropriate to criminalise it unless it 'seriously hinders' the functioning of the network and prevents other employees doing their jobs". R Downing, "Shoring up the Weakest Link: What Lawmakers around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime" (2005) 43 *Columbia Journal of Transnational Law* 705 at 729.

[69] *Morphitis v Salmon* [1990] Crim. LR 48.

running in the background, unless it causes a significant effect on the user's computer, should not constitute a criminal act. However, if the reports of other issues being caused are true, then those effects which cause a loss of functionality of a computer system (e.g. the loss of a CD drive) should be enough to satisfy impairment.

4.2.2. Mens Rea

The second aspect that needs to be proved is the *mens rea*, namely intention or recklessness and knowledge. As per s 3(1)(b) above, knowledge must be that the act was unauthorised. If there is no disclosure by a company of extra software then it follows that there should be knowledge that the act was unauthorised. The more complex issue of holding companies criminally liable will be discussed later.

Intention is unlikely to be apparent in the situation described. The intention must be for one of three possible outcomes following the act. They can be summarised as impairing the operation of the computer. Following the strict wording of the Act there is no need for this impairment to have happened, just that there was some intent to do so. In the SecuROM example there is a definite intention to do an act to a computer. But the act is intended to protect intellectual property, not to impair the computer's functions at all. The impairment, if it occurs, is just an incidental outcome from the act.

The original s 3 of the Act did not include recklessness. The addition of recklessness to the new offence was last minute and makes the scope far broader than if it was not included. With MacEwan suggesting that "[t]his [inclusion of recklessness] could prove to be a costly example of legislative overkill".[70]

There used to be two forms of recklessness; Caldwell[71] (objective recklessness) and Cunningham[72] (subjective recklessness). A full discussion of the history and development would not add anything to this article. So it is suffice to say that current law is from the case *R v G and another*[73] and the test is:

> A person is reckless if--(a) knowing that there is a risk that an event may result from his conduct or that a circumstance may exist, he takes that risk, and (b) it is unreasonable for him to take it having regard to the degree and nature of the risk which he knows to be present.[74]

Relating this to s 3 of the *Computer Misuse Act*, for a person to be guilty of the offence they must see a risk that their unauthorised act could lead to an impairment under s 3(2). In the case of the situation that has been dealt with there is obviously a risk that a computer will be slowed down by the DRMS, but as suggested above this should not be enough. There would have to be knowledge of a risk of some real impairment of a computer system. For example some of the problems that users have reported that they have encountered from SecuROM (e.g. CD drives not functioning). So for a case to be proved there would have to be some foreseeable risk that these

---

[70] N MacEwan, see note 66 above, at 964.

[71] *R v Caldwell (James)* [1982] A.C. 341.

[72] *R v Cunningham (Roy)* [1957] 2 Q.B. 396.

[73] *R v G and another* [2004] 1 A.C. 1034.

[74] *R v G per Bingham* LJ at 1047.

effects could happen. Issues could come up in testing that would lead to a foreseeable risk or, more likely after the problems complained of have been reported back to the company. There is always going to be a risk that something may go wrong, but again for criminal liability this would be unfair. That the specific effect should be foreseeable, for example the software maker must foresee the risk of CD drives not working etc.

4.2.3. Corporate Criminal Liability

The final thing that needs to be discussed is the ability of a corporation to be held responsible for a criminal act. To this end the article will turn to Working Paper 44 from the Law Commission which deals with "Criminal Liability of Corporations".[75] This neatly summarises the law on this issue. The general rule is that there are no legal barriers from bringing a criminal case against a company. Obviously there are certain offences that, due to their nature could never be committed by a company. The examples given in the working paper include rape, murder,[76] and bigamy. However it is only the nature of the offences that would stop criminal liability of a company. Liability can be found in two ways, either through vicarious liability[77] or through personal liability that is against the company as a legal person. It is the latter which is of most use here.

The *actus reus* of the offence is no more complex than if it was against an individual, and as has been shown above that has been satisfied in terms of s 3 of the *Computer Misuse Act*. The problems come with the *mens rea*, in the case in question recklessness. A company cannot have a sentient consciousness of its own. Its consciousness is made up of the sum of its constituent parts, its shareholders, directors, managers, and employees. So it needs to be proved that one of these constituent parts has the required mental state to commit the offence.[78] The next question is of course who to pick to represent the consciousness of the incorporated body. Here we can look to case law to help us:

> A company may in many ways be likened to a human body. It has a brain and nerve centre which controls what it does. It also has hands which hold the tools and act in accordance with directions from the centre. Some of the people in the company are mere servants and agents who are nothing more than hands to do the work and cannot be said to represent the mind or will. Others are directors and managers who represent the directing mind and will of the company and control what it does. The state of mind

[75] Law Commission (1972).

[76] There is also no possibility for holding a company liable where the only punishment available is imprisonment, which obviously cannot be applicable to a company. The only criminal punishment available will be a fine.

[77] Holding a company responsible for the acts of an employee or agent during the course of their job.

[78] It is unclear as to whether having the *mens rea* split between employees would result in liability, for instance one employee having the requisite knowledge and another having the recklessness to commit the accused crime. However, in the Law Commission's opinion this is unlikely to be the case.

> of these managers is the state of mind of the company and is treated by the law as such.[79]

This effectively restricts those able to give the company will to managers and directors who steer the company and make the decisions which could lead to committing a criminal act.

Could this allow for a computer games company to be held criminally liable under the *Computer Misuse Act*? That would depend on the how the company is set up. There needs to be at least one person in a position of authority who has the full *mens rea* for the offence, that person will likely either come from the legal or publishing departments. However, the legal person in charge of the licensing and thus the lack of authorisation must also know the nature of the DRMS that is being used. That it is a stand alone, self installing piece of software that should have its own disclosure in the EULA. The publishing manager will know which DRMS is being used, but will he know what is, and what should be, included in the EULA? Obviously the answer will likely be different depending on the size and structure of the company.

4.2.4. Suitability as an Alternative to Cyber-trespass.

Regardless, however, of the whether s 3 of the *Computer Misuse Act* is applicable to the situation described, it is unlikely to be suitable in practice. Criminal liability is unsuitable for mainstream computer companies selling cheap computer software to home users especially when the purpose of the questioned act is to protect intellectual property. The affected parties (home users) are unlikely to have the clout to get the CPS interested and it is unlikely the consumer ombudsman would be interested. The only remedy available would be a fine, and that is not helpful to those who have had their computers damaged by the software. Civil damages would be a far more appropriate remedy in this situation.

In essence, using the *Computer Misuse Act* as a basis for liability has its positive points. The *actus reus* of the offence should require some real interference with the computer system in question. This should be a higher threshold than for civil liability under cyber-trespass. So using Computer Misuse negates the potential problems with trespass to chattels being actionable *per se*. However the main drawback is the criminal liability that it is based on. This does not provide the best remedies for the parties affected by unauthorised access such as has been described. The remedy that fits best is compensation for the loss which has been suffered. A better approach would be to allow civil liability within the actus reus of the offence under the *Computer Misuse Act*. This will also allow for a lower threshold for damage, possibly along the same lines as the cyber-trespass law. This will be discussed in more detail later. But it is suffice to say here that pursuing this approach through the criminal courts is not a good alternative to cyber-trespass.

4.2.5. Cyber-Nuisance

Another alternative could be using the tort of nuisance as a better way forward. The Oxford *Dictionary of Law* defines nuisance as: "a tort, protecting occupiers of land

---

[79] *H.L. Bolton (Engineering) Co. Ltd. v P.J. Graham & Sons Ltd*. [1957] 1 Q.B. 159, per Denning L.J., at 172.

from damage to the land, buildings, or vegetation or from unreasonable interference with their comfort or convenience by excessive noise, dust, fumes, smells, etc."[80] Unfortunately, there is no such tort as nuisance to chattels; this means that real property rights would be required over computer systems. If this land aspect of nuisance could be avoided then this could be a promising avenue to follow. The "damage" that is caused in the unauthorised access cases which have lead to cyber-trespass being adopted would feasibly count as a nuisance. They are an "unreasonable interference" with the computer users "comfort or convenience" (mainly here convenience).

5. Conclusion

This article has tried to show the strengths and weaknesses of the cyber-trespass law created in America and has applied this to a real situation that is happening right now. However, it has shown that the US law would not be suitable for incorporation into the English system as there are key differences between the underlying law of trespass to chattels. The damage requirement is the key difference which makes the cyber-trespass rules incompatible and would lead to a very broad legal rule potentially covering too many digital situations.

The alternatives that I have suggested are quite mixed in their suitability. Nuisance would, to a certain extent, be a better fit, and in many ways cyber-nuisance would have been a preferable doctrine to cyber-trespass, but there is the real property hurdle in the way. For it to work well there would need to be a tort of nuisance to chattels which is not the case. Of the alternatives that exist at the moment the best is an action under the *Computer Misuse Act*. The main problem here being that criminal liability is not the ideal avenue in the situation I have described.

The best way forward is always going to be a specifically created law to deal with the question at hand. But this is not normally practical due to the differences in the pace of law and technology. Both cyber-trespass and computer misuse have their limitations. Cyber-trespass has its slightly murky past to contend with along with the issues of incorporation into English law. The *Computer Misuse Act* seems to tick all the boxes when it comes to the *actus reus*. It would do a good job in the circumstances of the current DRMS and its scope is broad enough to cover other uses of cyber-trespass. However its weaknesses lie in the *mens rea* and criminal nature of the offence. The obvious way of answering this question would be to combine the two. Tortious liability could have and should have been written into the *Computer Misuse Act* when it was created. The *actus reus* of s 3 of the computer misuse act requires damage, which I have shown to be a real issue when it comes to unauthorised access situations. It would solve the problems with the *Computer Misuse Act* and the unsuitability of its criminal sanctions. The problems that exist with the *mens rea* of s 3 of the *Computer Misuse Act* would also be solved by this solution. There are absolutely no issues with holding a company liable under tort. The standard asked of is also lower when it comes to *mens rea*. Negligence or just mere knowledge of an unauthorised act to a computer will likely suffice which would be far more likely in these situations. The level of damage could also be reduced to the level of the

[80] "Nuisance n." in J Law and E A Martin, see note 26 above, available at http://www.oxfordreference.com/views/ENTRY.html?subview=Main&entry=t49.e2639 (accessed 28 Mar 2011).

American cyber-trespass law after the Intel decision. As was discussed before, criminal liability should be based on a higher level of damage. All things considered this would be a preferable solution to the issues that I have discussed rather than incorporating cyber-trespass into the English system. It would also be a better solution than developing one of the other older torts to cover this area.