CYBER TRESPASS: A GOOD MODEL TO FOLLOW?

Should the English legal system adopt the US law on cyber trespass?

University of Oslo
Faculty of Law

Candidate name: Darren C. Read
Norwegian Research Centre for Computers and the Law.
Supervisor: Dr. Lee A. Bygrave
Deadline for submission: 21.09.2009

Number of words: 17,892 (max. 18,000)

21.09.2009

Contents

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 the new situations[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 old law on trespass to chattels. This gives computer system owners an action in tort when their systems have been accessed without authorisation. It enables them to receive compensation for any damage caused. However this has not been without controversy. The aim of this thesis will be to discuss whether or not the US law on cyber trespass should be incorporated into the English legal 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 contract, or creating a new civil offence designed specifically to deal with these situations.

There have been a few different activities that have lead to the US courts developing the law on 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 the restrictive Digital Rights Management Systems which are currently being used by the digital media industry, especially computer games publishers. In this thesis I will take Digital Rights Management Systems (DRMS) as a concrete example of where cyber trespass could come into play. More specifically I will

[1] For example see Lessig (2006) for a discussion on the US attempts to re-interpret the Fourth Amendment of the US Constitution when wire tapping became possible. Chapter 9 pg 157

look at the issues surrounding DRMS used to protect computer games. This will enable me to come up with some real conclusions about the necessity or attractiveness of incorporating this into the body of English law rather than keeping the discussion at a broad theoretical level.

1.1 Method

1.1.1 Focus

This piece of work will concentrate on the law in England and America. For the current cyber trespass laws I will have to look at American law as this is where it has been created and currently the only jurisdiction where such judicial creativity has occurred.[2] I will look at the current English law regarding trespass to chattels, comparing this with the general requirements under US law. Knowing the state of play before cyber trespass came into existence will enable me to look closer at whether it would work in English law. The other area of law that I will look at in depth is the Computer Misuse Act 1990 and show that this Act's provisions may provide an alternative, more tailor made, solution to the problem caused by DRMS such as those that I will look at. At times this piece of work will also mention other areas of law, for example contract law, further torts, and the laws relating to intellectual property, especially the law on Copyright. All these laws will be the law applicable to England, but may be English law or European law as incorporated by the English system.

1.1.2 Structure

To start off this piece of work I will give a brief introduction to DRMS and show how the problems they cause can lead to damage and thus a legal remedy being available. This will enable me to keep my discussions on cyber trespass and trespass to chattels more focussed

[2] Wong (2007) pg 91. This is further discussed in chapter 3 of this thesis.

from the outset. I will then go on to look at the cyber trespass law in detail; this will necessarily start with a comparison of the general rules that govern trespass to chattels in each jurisdiction. It will then look at the American law on cyber trespass as it has evolved to be. At the end of this section I will come to a conclusion over whether English law would be wise to adopt such a law. This conclusion will include both a general opinion over the quality of the law itself and then a more specific answer to the question of whether English law, with all its peculiarities, could and should successfully incorporate such a doctrine. In the final section I will look at alternative laws that have the potential to work better in the situation that I am discussing.

1.1.3 Approach

Although this thesis focuses partially on Digital Rights Management Systems (DRMS) this is not a piece of work on intellectual property law. It is firmly grounded in unauthorised access to computer systems and the potential liability this can attract. I am looking at DRMS as an issue in their own right without concentrating on what they are protecting. Although this will be mentioned in passing in chapter 2.

There is a paucity of secondary literature dealing with the issues at hand. Trespass to chattels has been discussed quite a bit since its inception at the beginning of the 21st century. But there hasn't been much discussion about it being exported to other jurisdictions, nor its applicability to DRMS. As far as I can tell there has been no discussion of the possible issues surrounding the use of cyber trespass where there is no physical connection between the two parties. So, to facilitate my analysis of the law I have relied heavily on the primary legal sources. I have used the growing body of case law as my point of departure for the discussion on cyber trespass in chapter 3. This necessarily follows the normal progression of case law as used by many other academics when describing the creation of the law. Chapter 4 is based mainly on statutory law, namely the Computer Misuse Act. Where such primary sources are unavailable I have utilised the

leading textbooks on the subject. This is the case with the discussion of trespass to chattels under English law, which, as I describe, is very poorly represented in primary law.

Other academics analyses will be used, but due to the freshness of my particular subject the conclusions that I come to are my own. This cannot be a piece of work built wholly or substantially on others' analysis, but on the primary legal sources themselves.

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. Representatives from these Industries have never been shy in outlining the effect this is having on the livelihoods of the employees in these industries. They maintain that the main threat comes from the internet and the ability to copy and share files with relative ease. To safeguard creativity and the cultural benefits creativity provides they are unanimous in their desire for more protection.[3] 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's impossible to come up with an exact assessment[4].

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. The choices that have been made have, to a certain extent, changed customer preferences. No longer do users simply buy their digital media for the cheapest price, but many actively

[3] For example see the entire published catalogue of Jack Valenti's (who was the president of the Motion Picture Association of America for some 38 years) opinions on the threat of piracy. Also see the MPAA's website for their views: <http://www.mpaa.org/piracy.asp>.

[4] The much publicised figures of $250billion monetary losses and 750,000 job losses, which can be found on the US Chamber of Commerce website <http://www.uschamber.com/ip>, 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/>. The Motion Picture Association of America (MPAA) has had to rectify one of its statistics as there was 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>. I won't go further into this as it is beyond the scope of this work.

seek out the most liberal anti-piracy measures they can as these give the user more freedom over the product they have purchased[5]. Nowhere is this more true 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.[6]

I will be concentrating on efforts to protect computer games and how these can fall foul of the law, most notably trespass to chattels. The computer game industry can be split into two sections, console games and PC games[7]. I will be concentrating on the issues surrounding PC games. PC games are more susceptible to unlawful copying due to the inherent nature of the PC. Consoles such as Microsoft's Xbox or Nintendo's Wii are designed specifically for playing video games. They have been created in such a way that makes piracy almost impossible, or at least unattractive. You won't find a copy function on a console, nor any way to write to a disc. Even though the new breed of consoles are internet ready and official content can be downloaded for free or at a cost[8] the ability to upload and download pirated games is unavailable. The proprietary nature of the platform means that it is very hard to create programs to enable such features as copying and sharing data. On the other hand copying and disseminating information are at the heart what a PC is for[9]. Couple this to the openness of the platform and the relative ease of creating programs and applications that run on them (such as cracks and hacks for protected programs) makes them a much more susceptible target for piracy.

Computer games publishers have had to attempt to find the balance between protecting their creations and keeping their customers happy. This balance is possibly even harder for computer games than for other media. There is more opposition to the measures taken by

---

[5] For example consumers purchasing DRM free music from Apples iTunes even though it is more expensive than the normal music tracks protected by Apples Fair Play DRMS, or even upgrade their current protected music for a fee, see <http://www.apple.com/pr/library/2007/04/02itunes.html>.

[6] One of the most notable is "Spore" released by Electronic Arts in September 2008. This will be discussed in more detail below.

[7] Throughout this piece when I say PC I will mean PCs and Apple Macs.

[8] For example using Xbox Live services or the Wii's market place.

[9] Made clear by the original Apple Slogan attached to their Macs "Rip, Copy, Burn"

computer games developers to protect their products than there have been for digital music downloads. The following four criteria can go some way towards explaining the opposing views that make the balancing act so hard:

- Production Costs: A computer game costs substantially more to produce than a typical music album, for example Spore is estimated to have cost EA in the region of USD$35million to develop (not including marketing or sales costs)[10]. This means the company will need better sales figures to recoup that money and start making profit. Compare this with figures of between USD$125,000 and USD$300,000 for producing a "popular album"[11]. Film production costs for blockbusters are huge but outweighed by the box office sales.[12]
- Expected Sales: The best selling PC game in history is The Sims produced by Electronic Arts, this has shipped 16million copies worldwide[13]. There have only been four games to have broken the 10 million mark, namely The Sims, The Sims 2, World of Warcraft, and StarCraft.[14] Contrast this to sales figures for music albums. The leading seller worldwide being Thriller by Michael Jackson with estimated sales of 109 million. There are over sixty albums with worldwide sales of over 20 million[15] which is more than any PC game has ever sold. DVD sales are less than with most music and games sales, but again these sales are secondary to the box office sales.
- Retail Price: Computer games retail at a far higher rate than music and a higher price than films (typically £30 to £40 for a PC game compared to £8 to £10 for a music album and £15 to £20 for a DVD) so the incentive to download an illegal copy is increased.

---

[10] <http://money.cnn.com/2008/02/12/technology/copeland_spore.fortune/index.htm>
[11] Vogel (2007) pg 162
[12] For highest grossing films see: <http://en.wikipedia.org/wiki/List_of_highest-grossing_films>, and for most expensive films see: <http://en.wikipedia.org/wiki/List_of_most_expensive_films>.
[13] <http://www.tmcnet.com/usubmit/2005/feb/1114806.htm> - these figures are from the release on feb 4th 2000 until 2005. However further sales will have been greatly reduced by the subsequent release of the sequels The Sims 2 and The Sims 3.
[14] <http://en.wikipedia.org/wiki/List_of_best-selling_PC_video_games>
[15] <http://en.wikipedia.org/wiki/List_of_best-selling_albums_worldwide>

- Computer Users' Protectiveness: Computer games affect a user's equipment more than other digital media. Whereas music and video files on a computer are only saved as files which are read by a media player, computer games, when installed, affect a far greater part of the system. Computer games dig deeper into the users' equipment and have the ability to affect it in unknown ways. The owners of computer systems will therefore be more selective when it comes to purchasing computer games and can be easily put off by anything which they see as either effecting their systems performance, or their control over it.

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.

This piece of work will discuss the DRMS option and will highlight this method using a current system as an example. This will put the discussion in some sort of real context and enable me to draw some real conclusions from the experiences of the discussed ideas rather than keeping the work hypothetical. I will use the SecuROM system as an example of a commonly used DRMS. This is a program which has caused some controversy over its scope and legality and will provide an example of DRMSs at their very strongest.

2.2 Digital Rights Management Systems

> *"Technological protections in the digital age take several forms, but all seek to provide a means for content owners to effectively dictate the permissible access to, and uses of, a work."*[16]

DRMS are pieces of code which restrict the use of a digital file in conjunction with the rights holder's wishes[17]. They are commonly attached to files protected by intellectual property law to enforce the rights holder's rights. Typical actions that DRMS restrict are copying, burning to CDs 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 those actions are illegal or not. Some well known DRMSs are Fair Play used by Apple to protect its protected music files available over iTunes and the CSS system which is commonly used to protect the contents of DVDs, stopping the DVD from being ripped to a computer and then distributed over the internet.

There has been some controversy over the use of DRMSs and the rights which they are being used to uphold.[18] They have the ability to protect far more rights than intellectual property law was ever designed to protect. As Lawrence Lessig puts it in his book Code v2:

> "An important point about copyright law is that, though designed in part to protect authors, the control it was designed to create was never to be perfect. As the Supreme Court noted, copyright "protection has never accorded copyright owner complete control over all possible uses of his work."[19] Thus, the law grants only particular exclusive rights, and those rights are subject to important limitations, such as "fair use," limited terms, and the first sale doctrine. The law threatened to

---

[16] Loren (2002) pg 134-5
[17] A more specific definition is impossible. Technology is always moving forwards and the types of protection invoked is continually changing.
[18] For some examples of these controversies see Adams (2006).
[19] *Sony* v. *Universal Studios, Inc.*, 464 U.S. 417, 432 (1984)

> punish violators of copyright laws—and it was this threat that induced a fairly high proportion of people to comply— but the law was never designed to simply do the author's bidding. It had public purposes as well as the author's interest in mind."[20]

DRMS have gone beyond that, they can now protect intellectual property perfectly. Fair use can be programmed out of a digital work (it is in fact much harder to program it into a work as fair use is subjective and can only be decided on a case by case basis). The first sale doctrine is also being eroded by the use of DRMS. Some systems only allow a product to be registered to a limited number of user accounts or to be installed on a limited number of machines. This makes resale either less valuable or worthless if the restrictions on the license have been used up. To a certain extent this has lead to many digital products being protected more by contract law than by copyright law. Most digital files will come with a comprehensive license agreement which sets out what the user may and may not do with the product. This means that they can easily contract out of exceptions to copyright which have been allowed for in legislation.[21]

The code nature of DRMSs means that they work in a different way to law based systems. Copyright and other intellectual property laws generally work *ex post*. That is to say that the law will become involve when a breach has occurred, the rights holder will likely be entitled to monetary compensation and the pirate may face other penal sanctions depending on the seriousness of the offence. Code based DRMS theoretically make it impossible to breach the rights holders rights in the first place, that is they work in an *ex ante* fashion. They are designed not to let such a breach occur in the first place. The law based system allows for a certain amount of wiggle room when it comes to enforcing rights whereas code based systems totally remove all possible discretion which can come from judicial decisions.

---

[20] Lessig (2006) pg 179

[21] There are some exceptions to actions that can be contracted out of. These are contained in the European Directives which I will mention later.

DRMS are not 100% secure right now. This has lead to a kind of arms race between computer game publishers and pirates. The publishers must try to keep at least one step ahead of the pirates and utilise stronger and stronger protection. However all the evidence suggests that they are losing this battle with the pirates. DRMS are susceptible to hacking. Commonly computer games which are protected by a DRMS have their protection cracked and pirated copies available within weeks; in some case within hours, or even before the game is officially released[22]. Therefore to protect the intellectual property better there have been many moves to strengthen the protection of the DRMS itself as well as the game. These protections go further than the copyright that the DRMS program would automatically acquire being, as it is, a computer program worthy of copyright protection. In the EU the protection of computer protection is governed by the Software Directive from 1991[23]. Article 7(1)(c) of the directive provides protection against commercial methods of circumventing DRMS. This has been incorporated into English law in s296 of the Copyright, Designs and Patents Act 1988[24]. Further European instruments such as the Information Society Directive[25] protect other forms of DRMS to a higher standard, but do not apply to computer software. They make it illegal to actually circumvent a DRMS rather than only commercialising a circumvention device. The provisions from this directive have been incorporated into English law in s.296ZA – s.296ZF of the Copyright, Designs and Patents Act 1988. Given the subject of this thesis a further discussion of anti-circumvention provisions isn't necessary.

[22] For example The Sims 3 was available 2 weeks before release :<http://www.edge-online.com/news/the-sims-3-leaked-online>.
[23] Directive 91/250/EEC on the legal protection of computer programs
[24] Copyright, Designs and Patents Act 1988 (C. 48)
[25] Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society

2.3 SecuROM

> *"SecuROM is the fastest growing and most effective copy protection system for CD-ROM and DVD-ROM"*[26]

SecuROM is a DRMS used by many computer game companies to protect their intellectual property from pirates. As can be seen from above it is advertised as the most effective and fastest growing such system. 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)[27]

SecuROM advertises itself as being capable of protecting from the three main types of piracy, namely 1 to 1 copying of a disc, the use of emulation tools which are programs that try to bypass copy protection, and the use of cracks which are modified applications with the copy protection removed.[28]

According to the SecuROM website the system achieves this level of protection by including a unique "uncopyable electronic keycode"[29] within the fabric of the CD or DVD itself when it is manufactured rather than after, which is the case with many other similar systems. This along with a software based authentication system allows access to the encrypted data on the disc. "The authentication mechanism is entirely key-less, meaning no serial numbers, stickers or artwork modification is required."[30] This is different to numerous other systems for copy protection which require a CD-Key be entered upon

---

[26] < http://www.securom.com/>
[27] 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>
[28] <http://www.securom.com/solution_general.asp>
[29] < http://www.securom.com/solution_concept.asp>
[30] See above no 29

installing the game, this key is usually printed either at the back of the user manual or on a separate sheet inside the game case.

The SecuROM system also gives the rights holder a large amount of scope over how they want to protect their game. The system enables three basic options each which can be fully customised. The rights holder can decide to use a disc based system whereby the CD or DVD is authenticated either upon every use, the first use, or after a certain number of uses or a selected period of time. There is also a time based system which can limit the time an application is used, or finally a usage based system which can limit the number of times a system can be used.

However, there is no mention on the website of the most controversial aspect of the SecuROM system. That is the way it installs itself on the computers of the computer game users. The program installs itself in the kernel of the operating system:

> "[T]he kernel is the central component of most computer operating systems. Its responsibilities include managing the system's resources (the communication between hardware and software components). As a basic component of an operating system, a kernel provides the lowest-level abstraction layer for the resources (especially memory, processors and I/O devices) that application software must control to perform its function. It typically makes these facilities available to application processes through inter-process communication mechanisms and system calls."[31]

Generally there is no warning that this is going to happen[32]. When this is the case the program is installed without any authorisation from the systems owner. It is this which can lead to an action under trespass to chattels which I will discuss later in this piece.

---

[31] < http://en.wikipedia.org/wiki/Kernel_(computing)>

[32] See the later discussion about the EA lawsuits relating to this system for more details.

This means that when installed on a computer system SecuROM is put straight at the top of the hierarchy of programs, even higher than the user themselves. All this without asking for or gaining permission from the owner of the computer system to be installed. When the owner of a system removes a game from their system which uses SecuROM the SecuROM program 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 program to remove SecuROM or follow a long and complex process which, if done incorrectly, could damage the system due to the location of SecuROM in the kernel.[33] All of this is very 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[34]. It was discovered by Mark Russinovich[35] that the system Sony were using had many similarities to spyware[36] and was effectively uninstallable without risking further damage to the computer system. The legal ramifications were never fully felt as Sony BMG settled the case by providing replacement CDs for all users who purchased infected products[37]. They have also released a program for uninstalling the DRMS.[38]

2.3.1 The EA Cases

Electronic Arts (EA) are the biggest computer game developer and publisher in the world. They have created some of the most notable computer game releases of recent time, for example The Sims franchise and the more recent game, Spore. They are one of the

---

[33] Process available here: <http://reclaimyourgame.com/index.php?option=com_content&view=article&id=68&Itemid=40>

[34] Scheier (2005)

[35] 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>.

[36] The encyclopaedia 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." Encyclopædia Britannica. 2009. Encyclopædia Britannica Online. 3 Sept 2009 <http://search.eb.com/eb/article-9471406>.

[37] Information of the settlement can be found here: <http://www.eff.org/cases/sony-bmg-litigation-info>

[38] Available at: <http://cp.sonybmg.com/xcp/english/updates.html>

companies that have opted to use SecuROM as their primary means of protecting some of their intellectual creations. The release of the computer game Spore created a certain amount of controversy. Spore was released on 4th September 2008[39] after a delay of well over a year. It is marketed as "your own personal universe. You can create and evolve life, establish tribes, build civilisations, sculpt worlds, and explore the cosmos."[40] When the game was released users were restricted to 3 installations of the game, this was increased to 5 installations after a number of complaints. The main complaint being what EA considered to be a new installation. Upgrading a computer could cost the user an installation, as could obviously buying a new computer. Sometimes, due to installation problems user used their entire limit without being able to use the game. Installations could be recovered by contacting EA and pleading your case to be allowed another. Now it is possible to do this online. [41] There was wide disappointment over the eventual product that was released mainly due to the use of SecuROM. For example users only gave it 4.5 out of 10 on the metacritic review website, compared with 84 out of 100 for professional critic reviews.[42] 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 22nd September 2008, just over 2 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.[43] This law suit has been 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. These have included a suit in relation to the computer game Mass Effect, and the Spore Creature Creator. I will now look at the case which Melissa Thomas filed against Spore. I will use this case as it was the first of the suits brought and is the most comprehensive with regards to the grounds on which it is brought.

---

[39] <http://eu.spore.com/whatisspore/platforms.cfm>
[40] See above number 39
[41] <http://eu.spore.com/whatisspore/article.cfm?id=32381>
[42]< http://www.metacritic.com/games/platforms/pc/spore?q=spore>. Figures correct as of 31st August 2009, although user score subject to change as more reviews are added.
[43] *Melissa Thomas* v. *Electronic Arts, inc.* Case 5:08-cv-04421-PVT

The crux of the cases is the inclusion of the SecuROM system as a “separately installed, stand alone, uninstallable DRM program”. And that this program isn’t 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 being:

> “A. Whether EA fails to disclose the presence of an additional program on the Spore gamedisk;
> B. Whether EA should have separately disclosed the presence of an additional DRM program on the Spore gamedisk, and the extent and nature of that program;
> C. Whether defendant should have disclosed, and is liable for its failure to disclose, prior to the purchase of the SecuROM program, the precise details and nature of the program, where and how it would install, and how it would operate, prior to any installation of the program;
> D. Whether defendant should have disclosed, and is liable for its failure to disclose, prior to the installation of the SecuROM program, the precise details and nature of the program, where and how it would install, and how it would operate, prior to any installation of the program;
> E. Whether the defendant should have obtain [sic] informed consent from the user, prior to the installation of the SecuROM program;
> F. Whether defendant concealed crucial details concerning the presence, operation, function, and uninstallability of the SecuROM DRM program to the class and the public;
> G. Whether defendants actions in concealing crucial details concerning the presence, operation, function, and uninstallabilty of the SecuROM DRM program were likely to deceive the public;
> ...

M. Whether by its conduct, defendant has trespassed on the computers of all persons who installed the Spore computer game;"[44]

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 I will be dealing with in this piece of work. Question M looks at trespass to chattels which will be the main discussion of this thesis.

Along with the pleadings in the lawsuit there have been many reports of the SecuROM system effecting users' computers in ways that is far from desirable[45]. It is a 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 isn't doing anything that the rights holder doesn't want them to do with their program. 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.

There have also been reports of DRMS stopping perfectly legal functions from working. For example in his paper "A Cost Analysis of Windows Vista Content Protection" Peter Gutmann outlines the collateral damage that emanates from Microsoft's attempts to protect premium content in its Windows Vista operating system:

[44] The brief for this case is available at <http://www.courthousenews.com/2008/09/23/Spore.pdf>
[45] 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>. 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.

> "Vista's content protection mechanism only allows protected content to be sent over interfaces that also have content-protection facilities built in. Currently the most common high-end audio output interface is S/PDIF (Sony/Philips Digital Interface Format). Most newer audio cards, for example, feature TOSlink digital optical output for high-quality sound reproduction, and even the latest crop of motherboards with integrated audio provide at least coax (and often optical) digital output. Since S/PDIF doesn't provide any content protection, Vista requires that it be disabled when playing protected content [Note E]. In other words if you've sunk a pile of money into a high-end audio setup fed from an S/PDIF digital output, you won't be able to use it with protected content. Instead of hearing premium high-definition audio, you get treated to premium high-definition silence.
>
> Say you've just bought Pink Floyd's "The Dark Side of the Moon", released as a Super Audio CD (SACD) in its 30th anniversary edition in 2003, and you want to play it under Vista (I'm just using SACD as a representative example of protected audio content because it's a well-known technology, in practice Sony has refused to license it for playback on PCs). Since the S/PDIF link to your amplifier/speakers is regarded as insecure for playing the SA content, Vista would disable it, and you'd end up hearing a performance by Marcel Marceau instead of Pink Floyd."[46]

There are also problems when it comes to video output as well as audio. Vista will disable any output that isn't protected, for instance component outputs won't work. Nor will most HDMI outputs even if they are sold as being protected. Premium content is generally HD or Blu Ray content which to gain the best results should be viewed using a much larger monitor than are generally used with computers. The most common method of using HD content on a computer would be to hook the computer up to a large HD ready Television by either a component cable or a HDMI cable. But if this doesn't work then having a HD or Blu Ray compatible computer for viewing movies is basically pointless (even more so if it is on a 15" laptop where the difference between HD and normal quality is negligible.)

[46] Gutmann (2007) available at <http://www.cs.auckland.ac.nz/~pgut001/pubs/vista_cost.html>

Unsurprisingly this feature of Vista is not advertised to users as it can be seen as punishing perfectly honest users from using functions which add to the viewing or hearing experience.

The problems surrounding the SecuROM system are even worse. Vista only stops HD playback of video and sound, but leaves the computer in general working order. SecuROM, on the other hand, has been known to affect the deep down functionality of the users' computer. For instance it can view having more than one CD or DVD drive as enabling piracy and therefore disabling one of them. Excluding laptops most computers sold nowadays have multiple disc drives as standard. There have been other reports of computers ceasing to function altogether after the installation of SecuROM.[47] It is these problems which will act as the point of departure for my discussion on trespass to chattels, and then of possible alternatives from other legal areas.

[47] These are, however, only reports of such things happening. The cause of the computer problems that some have experienced may not be down to the SecuROM software, but merely a coincidence that the problems started when they did. However, there are such a large number of reports that I would say that it is more than mere coincidence. See no. 45 above for concrete examples of such problems.

3 Trespass to Chattels

I will now dive into the murky depths of the law of trespass to chattels. This is a very old area of common law that has experienced something of a renaissance in The United States of America. However, the renewed interest in this area has not taken off in other common law countries yet[48]. This is because there have been no cases brought to the courts of any other jurisdiction yet where the claimant has relied on such a claim. This part of this piece of work will be split into three main parts. I will firstly look at the state of the law on trespass to chattels under English law, comparing and contrasting this to the general law in America before it was used in the digital environment. Then I 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 I 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. I will also apply the law to the examples in question on the presumption that the English courts would choose to borrow cyber trespass from the US.

[48] 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 anywhere but the US. This is also backed up by Wong (2006) pg 91

3.1 The state of the law

3.1.1 English law

Trespass to chattels (or trespass to goods)[49] is a very scarcely used law in the English legal system.[50] Because of this there is some ambiguity over the actual definition of the law and what is needed to succeed in a claim. However what is sure 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."[51] 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 some 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"[52]. In the case of *Leitch* v. *Leydon*[53] Lord Blanesburgh stated that: "The wrong to the appellants in relation to that trespass is constituted whether or not actual damage has resulted there from either to the chattel or to themselves."[54] However this would appear to only be *dicta* as trespass formed no part of the judgement in the end and

---

[49] 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. I 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.

[50] Following a simple case search on a law database it came up with 41 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.

[51] "trespass n." A Dictionary of Law. by Jonathan Law and Elizabeth A. Martin. Oxford University Press 2009 Oxford Reference Online. Oxford University Press. Oslo University. 31 August 2009 <http://www.oxfordreference.com/views/ENTRY.html?subview=Main&entry=t49.e4041>

[52] Heuston & Buckley (1998) pg 95

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

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

the discussion on English law was not technically applicable to this Scottish case. *Winfield & Jolowicz on Torts*[55] concurs with this interpretation of the law. The Oxford Law Dictionary also defines trespass as being actionable *per se*[56]. 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."[57] Looking at the various sources I would suggest that trespass to chattels doesn't require damage to be proved. All three forms of trespass, land, property (goods, chattels), and the person come from the same legal ancestry. There is no evidence that the courts have restricted the use of trespass to chattels to scenarios where damage was caused only, in fact the evidence suggests the contrary, following the opinion of most of the textbooks and Lord Blanesburgh in *Leitch* v. *Leydon.* As I will show in the next section, it is being actionable *per se* in English law that sets it aside from the law in America. This difference could prove a large stumbling block when it comes to the potential incorporation of cyber trespass into English law.

It is worth noting here that the Torts (Interference with Goods) Act 1977 has gathered together all the various tortuous property offences (such as trespass to chattels and conversion) under the umbrella term of wrongful interference. This act only deals with procedural aspects of the law such as remedies. It doesn't change the offences themselves[58] and the old case law and definitions of the various offences remain the correct law.

[55] Rogers (2002)
[56] "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." Supra number 51
[57] Deakin et al (1999) pg 407 as quoted in Wong (2007)
[58] Except for the abolishment of the offence of detinue in Section 2 of the act

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) section 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.

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."

Compare this to the state of the English law above. As I mentioned there the requirement for damage is a striking difference between the two systems. I will discuss the importance of this difference after I have laid out the law on cyber trespass.

3.2 Cyber- trespass

> *"[W]hat we are now observing in the context of the Internet is not only a new form of proprietary interest, but no less than the emergence of a new form of intellectual property, with only the most tenuous of antecedents in the law of chattels."*[59]

It was in relation to telecommunications that trespass to chattels was first used to deal with technological issues. In Thrifty *Tel* v. *Bezeneck*[60] the plaintiffs were held to be liable under trespass[61] after hacking into the long distance telephone network of thrifty. 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 obviously hurdles which had to be jumped before a claim would 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 found 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 by the courts.

The courts in thrifty decided that the chattel that was being trespassed upon was the phone network[62], this brought trespass to chattels into play. The problem then was the physical contact. There was no physical contact by the plaintiffs to the network. They didn't go to an old fashioned telephone exchange and start moving wires around themselves; they were doing it from afar trying to get into the system by "phreaking"[63]. The courts decided that the electronic signals that the plaintiffs were creating and "touching" Thrifty's network were "sufficiently tangible to support a trespass cause of action". In this case the idea of

---

[59] Burke (1999) pg 2
[60] *Thrifty Tel* v. *Bezeneck* 54 Cal. Rptr. 2d 468 (Cal. Ct. App. 1996)
[61] Incidentally Thrifty was originally trying to prove conversion, but it was the courts that substituted the conversion claim for one of trespass to chattels. So this whole body of law started in a case where the claimants were not intending to rely upon it.
[62] I briefly discuss whether trespass to land would have been a better tort to base this on. This is in section 4.3.
[63] A portmanteaux word created from "phone" and "freak". For more information see <http://en.wikipedia.org/wiki/Phreaking>

damage was given only a cursory mention, but was held to be apparent from the facts so the claim succeeded. The idea of damage was, however, to be further discussed in subsequent cases.

This case was followed by the Ohio courts in the first case which dealt directly with computers and computer networks. This was as a response to spam and was before the US CAN-SPAM Act (2003) can into force which provides custom built legal protection against spam. In *Compuserve* v. *Cyber Promotions*[64] Compuserve sued Cyber Promotions for damages after they had sent a multitude of spam emails to its customers. The court followed the reasoning in Thrifty when it comes to the physical contact that trespass necessitates, electronic signals are enough to constitute such a touching. The damage here was, controversially, not just to the system that was touched. The court decided that the damage could have been a couple of things. 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 section 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, merely the value of it as a whole.[65] 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 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 doubtful. The whole reasoning behind damage has been criticised by many in the academic world especially from Dan Burke in his article "The problem with trespass".[66]

> "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

[64] *Compuserve* v. *Cyber Promotions* 962 F. Supp. 1015 (S.D. Ohio 1997)
[65] *Compuserve* v. *Cyber Promotions*, per Graham, District Judge at 1021-1022
[66] Burke (1999)

> 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."[67]

There has been a whole raft of similar cases going through the courts in America since the groundbreaking Compuserve decision. The most notable being *eBay* v. *Bidders Edge*,[68] a number of cases involving America Online (AOL)[69] and *Register.com, Inc* v. *Verio, Inc*[70]. All of which have had to grapple with the idea of what constitutes damage. In doing so they have managed to come to some rather dubious decisions. 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 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. Here it was clear that the courts wanted to dissuade other "free-riders" from making money out of someone else's work (in this case eBay's popular auction website).[71] In Register.com the plaintiff was trying to stop the defendant (Verio) from using its WHOIS database without permission by sending lots of emails requesting information. This was after they had tried

---

[67] Burke (1999), Pg 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.

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

[69] *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).

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

[71] How this decision would affect the myriad of price comparison sites is up for discussion here. For example sites which compare car insurance prices from different insurance companies requiring the user to fill in just one form. They use similar methods as Bidder's Edge to conglomerate the information. This could arguably result in a claim under trespass in the US, but I doubt that it would be in the interests of any of the insurance companies. Basically it is a new way of gaining customers and should be viewed as being advantageous rather than as a bad thing.

to negotiate a license to use the database but had been rejected. 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 for further cases.

The final case in the creation of cyber trespass is *Intel* v. *Hamidi*[72]. This case involved an unhappy employee (Hamidi) of Intel who, after leaving the company[73], 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 this was held to be a trespass. Although Intel was not a service provider so the emails on the system couldn't affect customer goodwill the time taken by the employees to sift through Hamidi's (not too frequent) emails was held to be enough to find damage. Staff also took some time to try and 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 and thus a trespass. This case, unlike the previous ones, didn't really have a good policy reason for the decision. The emails weren't anywhere near the quantities of the other Spam cases[74]. 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 the 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

[72] *Intel corp.* v. *Hamidi* First decision: 114 Cal. Rptr. 2d 244 (2002), reversed by: 30 Cal. 4th 1342 (2003)
[73] Either fired <http://www.cnn.com/TECH/computing/9905/03/emaillaw.idg/index.html> or left due to work related injury <http://www.wired.com/news/news/politics/story/19395.html>.
[74] There were six mail shots over a period of 2 years. *Intel* v. *Hamidi* per Werdegar, J. at 1346

> 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."[75]

This decision has attempted to reign in the scope of cyber trespass in the US courts. Although, obviously not binding precedent in the other states, it is a persuasive argument and arguably correct interpretation of the law. Only damage to the computer system itself can lead to an action in trespass. As Burke puts it "employees are not chattels"[76]. 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. This seems to bring cyber trespass back in line with the law as set out by the restatement of torts.

All of the above cases have dealt with email or screen scraping. The situation I am looking at is slightly different. The situation involving SecuROM and other similar DRMS involve the secret installation of software. This type of compliant has been the subject of some later cases; most notably *Sotelo* v. *DirectRevenue*, *LLC*[77]. This case involved the secret bundling

---

[75] *Intel* v. *Hamidi* per Werdegar, J. at 1347
[76] Burke (1999) pg 11
[77] *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 are preliminary hearings

and installation of spyware[78] 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 made no difference to the claim, which makes sense. There is no conceivable reason why trespass can only be against a large network. In response to the plaintiffs' request for dismissal of the claim of trespass the courts used the Compuserve reasoning when it came to deciding what constitutes damage[79]. 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. Although this secretly bundled program comes on a game disc rather than downloaded over the internet, this should make no difference when it comes to damage under trespass, but may cause a problem when it comes to the physical touching, this I will discuss in the next paragraph. However, once more, there are strong policy reasons behind this decision. Spyware is a bad thing and any means to help get rid of it is most welcome. But this can't really be said about DRMS. They are not programs 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. Would the court have come to the same decision if the activity claimed over wasn't as abhorrent as spyware?

---

where the courts dismissed the defendants' claims to dismiss. There have been no final rulings at the time of my writing.

[78] In his article Mathias Klang gives a good 4 point definition of spyware. Klang (2003) pg 314

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

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 reasoning is somewhat fluffy. As I have mentioned before the reason for this fluffy logic was most likely due to policy reasons, stopping an unwanted behaviour from continuing. But as Burke has argued it is stretching the definition of physical to its very limit[80]. It could arguably need stretching even more when the software complained of is stored on a disc rather than coming down the network wires. There is no physical connection for the electronic signals to travel down between the two systems. There is never a direct physical link from the plaintiff to the claimant. 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 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 program 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[81]. This would suggest that an indirect physical intermeddling such as using a disc would fit within this definition. Unfortunately there is no case law on this matter, it will have to be decided upon in the SecuROM cases involving EA if they ever get to court, but as of now there is no precedent. In my opinion, although there is no direct physical contact it would seem unjust to only be able to apply cyber trespass where there is the direct internet link. The analogy of throwing an object to damage a chattel is valid in this situation.

[80] See above no. 67
[81] Comment e. of Restatement (second) of Torts s.217.

3.3 Incorporation into English law?

As I have discussed above trespass in English law is likely to be actionable *per se*, that is no damage needs to be proven for a remedy to be awarded. This is not the case in American law. Originally the damage requirement for cyber trespass was interpreted very (too) 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 wasn't having a real detrimental effect to eBay's computer system. Register.com's system wasn't 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 shouldn't 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 there would be a real problem that cyber trespass would overreach. The number of situations where it would be potentially applicable would be far too many 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 *per se*. 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 cyber trespass would be an unwelcome addition to the English law.

Where the American law doesn't mention the need for a direct contact, just a physical one, it would appear from the definition of the English law that this may not be the case in England. The definition in the Oxford legal dictionary calls for a "wrongful direct interference with... goods"[82]. 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? Does there have to be any direct physical connection between the plaintiff and claimants property? 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. This potential problem is not as serious as the issues surrounding damage that I have described above. It doesn't stop trespass to chattels being used in England to deal with similar cases such as the American cases. It would however, potentially make it not applicable to the DRMS scenario I have outlined. But it wouldn't be beyond the scope of judicial creativity to reinterpret the law in such a way.

So, overall, cyber trespass does have some positive aspects. Since the Intel decision it has been brought under control to make a practically applicable law that deals with the situations well. Whatever its theoretical background it is a good law that should be commended. It would not, however, be a good idea to incorporate it into the English system with the law on trespass to chattels as it currently is. The damage aspect of English law is a large barrier which I would suggest would be insurmountable. Cyber trespass without the limiting factor of requiring damage would not be good law.

[82] Above, no. 51

4 The Alternatives

There are alternatives to incorporating a trespass to chattels approach into the English system. I will look at alternatives under criminal law first and then mention some options under contract law. I will also look at possible alternate torts that a cyber trespass type law could be based on. After that I will suggest that rather than using cyber trespass the English system should amend the computer misuse act (which I will look at below) to include some tortuous liability as well as criminal liability. As I will show, the fact that the computer misuse act only deals with criminal liability is its major weakness as an alternative to cyber trespass.

4.1 Criminal Law

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."

Section 10 of the act sets out what is to be considered as property with regards to criminal damage. Unlike with theft[83], property is restricted to tangible property, be it real or personal,[84] so it can be land but not something intangible or a "thing in action". The cases of *Cox* v. *Riley*[85] and *R* v. *Whiteley*[86] made it clear that this didn't 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 section 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."[87]

This provision has now been moved to section 10 of the Criminal Damage Act following the Police and Justice Act 2006 schedule 14. This act amended the Computer Misuse Act quite considerably, which I will come to now.

4.1.1 Computer Misuse Act 1990

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

[83] Theft Act 1969 s.4
[84] S.10 Criminal Damage Act
[85] *Cox* v. *Riley* (1986)83 Cr. App.R.54
[86] *R* v. *Whiteley (Nicholas Alan)* (1991)93 Cr. App. R. 25
[87] S.3(6) Computer Misuse Act 1991 before amended by Police and Justice Act 2006

covered by the act; unauthorised access to a computer system[88] and unauthorised modification of computer material[89]. There is also a third offence which is unauthorised access with intent to commit a further offence, in essence an aggravated form of the s.1 offence.[90] I will now look at each of the offences in turn, starting with a brief look at s.1 and then a more detailed look at the s.3 offence.

4.1.1.1 Computer Misuse Act s.1

Many programs "phone home" to their creators with information about the system which they are being used on. This can be used by the company in a multitude of ways, for instance research on what systems people are using their programs are on, or, in the case of a lot of 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 used on, such as the operating system.

Section 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, Section 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

---

[88] S.1 Computer Misuse Act

[89] S.3 Computer Misuse Act. 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.

[90] S.2 Computer Misuse Act

(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[91]. However it has a broader scope than simply protecting against the archetypal hacker, that is someone sitting at home with a personal computer, whether with malicious intent or not. It can go further to protect any unauthorised access to computer data which means it can potentially be used with reference to perfectly legitimate computer programs 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 authorisation or otherwise. If there was included in the license agreement pertaining to the program a clause which sets out that the program 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.

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

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."

Section 2 of the act provides for stricter penalties if the unauthorised access was done with the intent to go on and commit a further offence, this further offence must be punishable by more than 5 years imprisonment[92]. There is no scope for this to be used in any circumstance that I am looking at.

4.1.1.2 The Old Computer Misuse Act s.3

Before it was replaced by the new section 3 offence by the Police and Justice Act 2006 section 3 of the Computer Misuse act set out the offence of "unauthorised modification of computer material"[93]:

"(1) A person is guilty of an offence if—

(a) he does any act which causes an unauthorised modification of the contents of any computer; and

(b) at the time when he does the act he has the requisite intent and the requisite knowledge.

(2) For the purposes of subsection (1)(b) above the requisite intent is an intent to cause a modification of the contents of any computer and by so doing—

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer; or

[92] Section 2(2)

[93] I am mentioning this because the new offence came into force in October 2008, after the use of SecuROM in some cases, thus making this the applicable law rather than the new offence. There is also substantial overlap between the two offences. The new offence expands on this offence, but anything that was unlawful under the old law will still be caught by the new offence.

(c) to impair the operation of any such program or the reliability of any such data.

(3) The intent need not be directed at—

(a) any particular computer;

(b) any particular program or data or a program or data of any particular kind; or

(c) any particular modification or a modification of any particular kind.

(4) For the purposes of subsection (1)(b) above the requisite knowledge is knowledge that any modification he intends to cause is unauthorised.

(5) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it of a kind mentioned in subsection (2) above is, or is intended to be, permanent or merely temporary."

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

For the first question s17 on interpretation is of great help. S17(7) states that:

> A modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer—
>
> (a) any program or data held in the computer concerned is altered or erased; or
>
> (b) any program or data is added to its contents;
>
> and any act which contributes towards causing such a modification shall be regarded as causing it.

So, for instance, placing a program on a computer would fit as a modification to the system 17(7)(b). This has to be done using that computer, or another computer, which would seem to cover all areas. Authorisation is also dealt with under s17 of the act, more specifically s17(8):

> Such a modification is unauthorised if—
>
> > (a) the person whose act causes it is not himself entitled to determine whether the modification should be made; and
> >
> > (b) he does not have consent to the modification from any person who is so entitled.

As Neil MacEwan puts it: "If the accused was not entitled to control the process in question (access or modification/impairment), and did not have the consent of someone who was, the requisite lack of authority is established."[94] This is a simple test of authority that would exist in any realm of life, be it electronic or with regards to real property.[95]

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 DRMSs being utilised. But since there is nothing to tell 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 I think that this line of argument would, and should, ultimately fail. Here it is useful to use the analogy from the comment on *DPP* v. *Bignall*[96]: "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." The user may give authorisation for the use of DRMS to protect a company's intellectual property, but it doesn't follow that this authorisation is for the installation of a stand-alone program which is placed at the heart of the computer system and cannot be (easily) uninstalled even if the game is uninstalled.

---

[94] MacEwan (2008) pg 957
[95] For an in depth discussion of the meaning of authorisation see Kerr (2003)
[96] *DPP* v. *Bignall* [1998] 1 Cr. App. R. 1

The second aspect that needs to be proved is the mens rea, namely intention and knowledge. As per S3(4) 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 must be knowledge that the modification is unauthorised. Intention is much harder to find following the wording of the act. The intention must be to make a modification, which again is easy to find in cases such as the SecuROM example. There is a definite intention to install the DRMS without the consent of the users, thus satisfying both knowledge and intent thus far. However there it would appear that there must also be intent to go on and cause a further act. The three actions which must be intended can be basically summarised as impairing the functionality of the computer. Computers can easily be impaired following the installation of software, authorised or unauthorised, but the intent will rarely, if ever, be there. The intention of DRMSs is to protect intellectual property by stopping piracy. The Vista example above is to stop the copying of protected High Definition music and videos; with DRMSs attached to computer games, amongst other things, to stop the games being shared online. There should (hopefully) be no intention to impair the use of the users' computer, whether this happens to be a side effect or not. So an honest company (honest in terms of the intention of their protection simply to protect) will not be liable under the old section 3 of the Computer Misuse Act.

There are also some problems when it comes to defining what an impairment is. 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. In the American law of trespass to chattels it would appear that simply using up some of the processing power of the computer is enough to lead to liability through the tort[97]. This has lead to quite a wide definition of impairment which includes a noticeable drop in performance. 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. 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

[97] See my discussion in 3.2

negligible. In *Morphitis* v. *Salmon*[98] for example a scratch on a scaffolding pole was held not to constitute criminal damage as it didn't affect the usefulness of property. If such a principle was used by the courts to decide if any intended impairment was enough to lead to a liability under the Computer Misuse Act then simply using processing cycles and memory should not be enough. Unless there are many programs that have been installed or the program is particularly resource hungry it would be unreasonable to infer criminal liability there from. In, for example, the SecuROM example there is evidence that the program has caused all sorts of havoc to users systems including restricting access to perfectly lawful programs already installed[99]. This, in my opinion, would be more than a minimal interference and therefore liability should be able to arise under those circumstances.

4.1.1.3 Computer Misuse Act s.3 as amended by Police and Justice Act 2006

This section 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 section 3. In fact in the case of *DPP* v. *Lennon*[100] the court of first instance decided that a denial of service attack perpetrated by sending millions of emails was not contrary to section 3. The (somewhat flawed) logic behind the decision was that since the company that was attacked had an email server which was 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

[98] *Morphitis* v. *Salmon* [1990] Crim. L.R. 48

[99] This also brings up the causation and the need for evidence to prove that the damage/impairment was actually caused by the company's actions. Problems with users' computers could merely coincide with the installation of the software in question but not be caused by it. This is a question of fact that would have to be decided on a case by case basis and cannot be satisfactorily answered in this piece.

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

reheard, but the confusion over the status of denial of service attacks was enough to get the government to review the law and make the following amendments.

Section 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;
> >
> > (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 actus reus of this new offence is now simply doing an unauthorised act to a computer. This is simpler than the old actus reus of needing to have modified the computer in some way. This means that this new section has a broader scope which encompasses all the cases which would have fallen under the old offence, but will also include more situations, as the government intended. Looking at the situation in question, as I showed that it fitted into the old section then there will be no problem when it comes to applying the new section. Installing a program is doing an act, and as stated above this act can be unauthorised if there isn't proper disclosure as to the nature of the installation.

The main relevant difference between this offence and the old one is the mens rea of the offence. Knowledge is still there, but now, as well as intention, recklessness will suffice to make a party liable. As with above there still won't be any intention for the same reasons. Companies will not be making programs which are intended to stop their customers' computers from working. But the inclusion of recklessness in the new provision has opened a potentially more promising avenue. 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."[101]

There used to be two forms of recklessness; Caldwell[102] (objective recklessness) and Cunningham[103] (subjective recklessness). A full discussion of the history and development wouldn't add anything to this thesis so I will go straight to the law as it is now. That current law is from the case *R* v. *G and another*[104] 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

[101] MacEwan (2008) pg 964
[102] *R* v. *Caldwell (James)* [1982] A.C. 341
[103] *R* v. *Cunningham (Roy)* [1957] 2 Q.B. 396
[104] *R* v. *G and another* [2004] 1 A.C. 1034

> unreasonable for him to take it having regard to the degree and nature of the risk which he knows to be present."[105]

Relating this to s.3 of the Computer Misuse Act that I have been describing, 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 I have been dealing with there is obviously a risk that a computer will be slowed down by the DRMS. But as I have suggested above this shouldn't be enough for criminal liability to arise. 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 encountered from SecuROM (CD drives not functioning etc). So for a case to be proved there would have to be some foreseeable risk that these effects could happen. Issues could come up in testing that would lead to a foreseeable risk. There is always going to be a risk that something may go wrong, but again for criminal liability this would be unfair. I would argue that the specific effect should be foreseeable, for example the software maker must foresee the risk of CD drives not working etc.

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 I turn to Working Paper 44 from the law commission which deals with "Criminal Liability of Corporations"[106]. 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,[107] 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

---

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

[106] Law Commission (1972)

[107] 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.

ways, either through vicarious liability[108] or through personal liability, that is against the company as a legal person. It is the latter which is most use here.

The actus reus of the offence is no more complex than if it was against an individual, and as I have shown above that has been satisfied in terms of s.3 of the Computer Misuse Act (as amended). 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 and therefore intention are 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[109]. 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 of these managers is the state of mind of the company and is treated by the law as such."[110]

This effectively restricts those able to give the company will to those at the top. That is managers and directors who steer the company and make the decisions which could lead to committing a criminal act. In the leading case of *Tesco Supermarkets Ltd* v. *Nattrass*[111] it

---

[108] Holding a company responsible for the acts of an employee or agent during the course of their job.
[109] 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 or intention to commit the accused crime. However, in the law commissions' opinion this is unlikely to be the case.
[110] *H.L. Bolton (Engineering) Co. Ltd*. v. *P.J. Graham & Sons Ltd*. [1957] 1 Q.B. 159, per Denning L.J. at 172
[111] *Tesco Supermarkets Ltd* v. *Nattrass* [1972] A.C. 153

was held that even a branch manager could be the conduit through which liability could pass, although on the facts of the case it was held otherwise here.

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. In terms of a computer games company (most likely the publisher as opposed to the developer as they will deal with the practical aspects of getting the game onto a disc and related jobs such as the copy protection) that person will likely either come from the legal department or from the publishing department. 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. This area of uncertainty would make action under the Computer Misuse Act risky and therefore less suitable for use in such cases.

Regardless, however, of the answer to the questions posed, this line of attack is unlikely to ever come to fruition. The offence itself, as perpetrated by mainstream companies selling reasonably cheap computer software to home users, is far from serious enough to get the state involved in prosecuting a company. The only remedy available would be a fine for the company involved, and depending on how the case is brought this could be a minimal. If it was decided that it was a single offence then the fine could only reach a maximum of £5000. If it is decided that each computer that has become broken is a separate offence then obviously the fine could be greater. But evidentially there would be a problem with what actually caused the impairment of the system. There is also going to be major issues with coming to an accurate number of people affected by the system which has caused the problem. Arguably there would more likely be a case brought if the victim was a large public body, or a series of large companies where the damage involved was massive (rather

than the seemingly insignificant amount for a home system). But in these cases contract law would likely be involved as with contracts that size there would inevitably be clauses regarding any damage.

There would also be little to instigate a private prosecution from an individual, or group of individuals, using the criminal law. There would seem little point in going through the criminal courts, with the higher burden of proof, to get the company fined. The alternative would be to go through the civil system with its lower burden of proof and the prospect of compensation.

In essence, using the Computer Misuse Act as a basis for liability has its positive points. The actus reus of the offence requires some real interference with the computer system in question. Although there is no case law yet on what would amount to an interference I have hypothesised that it should follow other criminal law provisions such as criminal damage. This should be a higher threshold than for civil liability under cyber trespass. This would be harder to prove than the damage test under Intel, which is a fair test under civil liability. 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 doesn't provide the best remedies for the parties affected by unauthorised access such as I have 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 offense 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. I will discuss this 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 Contract Law

4.2.1 Misrepresentation[112]

A misrepresentation is an "unambiguous false statement of facts which is addressed to the party misled and which induced that party to enter into a contract"[113]. It is helpful to again split this into separate aspects which need to be satisfied to find a misrepresentation. These are (1) unambiguous (2) false (3) statement of facts (4) which induced that party to enter into a contract.

There is no general duty in English contract law to disclose information[114], but misrepresentation can arise if some information is given, but not the whole story. In *Arkwright* v. *Newbold*[115] James LJ stated: "supposing you state a thing partially, you may make a false statement as much as if you misstated it altogether. Every word may be true, but if you leave something out which qualifies it you may make a false statement."[116] Even more helpful for the problem in question is the case of *Dimmock* v. *Hallett*[117] where a farm was sold as fully tenanted. However the seller failed to disclose the fact that, although this was true at the time, the leases were not going to be renewed when they expired. It was held here that it was a misrepresentation as there was only a partial disclosure of the facts. If there had been no disclosure at all regarding the status of lease situation then there could have been no misrepresentation.

This area of law can only be of use in certain circumstances depending on the companies' use of the systems in question; it does not really affect the legality of the system itself, only its implementation. In the case with EA it was disclosed that there was a DRMS in use with

---

[112] A full discussion on misrepresentation will not add too much to the discussion as it is not directly linked to the software being used, but the contract under which it is being released. For a full discussion see: McKendrick (2003)
[113] McKendrick (2003) pg 630
[114] *Keates* v. *Cadogan* (1851) 10 CB 591
[115] *Arkwright* v. *Newbold* (1881) 17 Ch D 301
[116] *Arkwright* v. *Newbold* per James LJ at 318
[117] *Dimmock* v. *Hallet* (1866) LR 2 Ch App 21

the Spore game. This was stated on the packaging, which also specifies the need to have an internet connection to register the game. It is also stated in a Q&A page on EA's customer support website[118]. There is no mention anywhere that the DRMS in question is a standalone program that will be installed onto the users system without their knowledge or authentication. Using the *Dimmock* case to illustrate this situation, revealing that a DRMS is being used with the game is akin to saying that the farm being sold is fully tenanted. However not revealing that this DRMS is in fact a separate program with the qualities which SecuROM has is not revealing that the leases have not been renewed. I would say, therefore that there has been a factual misrepresentation in such a situation as there has only been partial disclosure, the whole nature and quality of the system being used has not been disclosed to the purchaser of the program. Perversely, because it has been disclosed that there is some DRMS in use this leaves the company open to a claim under contract law. If they had not disclosed anything about the protection measures they have taken then there could be no action here. Since I have shown that there is a misrepresentation it must be shown that this induced the claimant into entering into a contract. In essence the question must be that if the customer knew that the DRMS being used was a standalone system which would run on their system at all times and would be uninstallable (as it was originally) or very hard to uninstall (as it is now) then would they have gone on to purchase the game? This is obviously a subjective question which would have to be decided on a case by case basis as different users would weigh up the options differently. But it is clear from some users' comments and reviews on the game that they would not have bought the game if they had known the whole story. Others, following those comments have in fact gone on to not purchase the game.

---

[118] Available at: <http://support.ea.com/cgi-bin/ea.cfg/php/enduser/std_adp.php?p_li=&p_sid=rapS**Ej&p_sp=&p_faqid=19743&p_iid=0&p_created=&p_prod=&p_cat=&p_cv=&p_pv=&p_prods=&p_cats=&prod_lvl1=&prod_lvl2=&prod_lvl3=&cat_lvl1=&cat_lvl2=&cat_lvl3=&p_hidden_prods=&p_search_text=&p_new_search=&p_accessibility=&p_page=&p_lva=19743&nextlink>

4.3 A New Approach?

Cyber trespass has been based on the old law of trespass to chattels. But some have suggested that it seems more like the law on trespass to land[119]. The idea being that it could iron out some of the theoretical difficulties involved. Using trespass to land as a basis for governing unauthorised access to computers would involve granting real property rights to cyber space. This could be a counter-productive approach which could lead to restrictions on the internet which wouldn't be beneficial to society as a whole [120] . Although it could help with some of the theoretical problems with the current cyber trespass law it would cause some practical problems. Trespass to land is actionable *per se* in both England and the US, so basing the law on this would fail to iron out the damage issue in English law and would create a damage issue in the US. So overall, this approach would fail to improve on the weakness experienced by the trespass to chattels approach in English law and would make the situation even worse in the US. For these reasons I would contend that it would be a poor choice of laws on which to base such a doctrine as cyber trespass. It would not be worth the problems that creating real property rights in cyberspace would make as there would be no real practical benefit from it.

Another alternative could be using the tort of nuisance as a better way forward The Oxford Law Dictionary defines nuisance as: "a tort, protecting occupiers of land from damage to the land, buildings, or vegetation or from unreasonable interference with their comfort or convenience by excessive noise, dust, fumes, smells, etc."[121] . This would again require computer systems to be classified as real property, which as I suggested above, would open a whole new can of worms. There is no such tort as nuisance to chattels. If the land aspect of nuisance could be avoided then this could be a promising avenue to follow. The

---

[119] See Burke (1999)

[120] This is a view held by Harold Smith Reeves in his article "Property in Cyberspace", Reeves (1996).

[121] "nuisance n." A Dictionary of Law. by Jonathan Law and Elizabeth A. Martin. Oxford University Press 2009 Oxford Reference Online. Oxford University Press. Oslo University. 8 September 2009 <http://www.oxfordreference.com/views/ENTRY.html?subview=Main&entry=t49.e2639>

“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

In this piece of work I have tried to show the strengths and weaknesses of the cyber trespass law created in America and have applied this to a real situation that is happening right now. The law of cyber trespass could be seen as an example of judicial overreaching. Taking an old legal rule and distorting it beyond recognition to deal with new technological situations. But since the decision in *Intel* v. *Hamidi* the law has been brought back into line with its origins. It is now a useful doctrine for the American system which deserves a place in the US body of law. However, I have also 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 possible problem with the American judges' interpretation of touching is another potential problem, but not insurmountable due to the vagueness of the actual legal rules in England.

The alternatives that I have suggested are quite mixed in their suitability. Trespass to land is a definite no go considering the implications of considering cyber space akin to real property. It also fails to deal with any of the pitfalls regarding damage that I have identified. Nuisance would be a better fit, and in many ways cyber nuisance would have been a preferable doctrine rather than cyber trespass, but again 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 doesn't exist. Contract law is always going to be an option where there is a badly drafted EULA. It also has the ability to prescribe the correct remedies. But it is quite easy for a computer games publisher to avoid contractual liability by better drafting. This drafting could either negate all the issues with disclosure, therefore making unauthorised

access authorised, or could mean no disclosure at all. For this reason it's not a great alternative to cyber trespass. Of the alternatives that exist at the moment the best is an action under Computer Misuse legislation. 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 DRMSs 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 American cyber trespass law after the Intel decision. As I discussed before, I would argue that 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.

References

List of Judgements/Decisions

English Judgements

Arkwright v. *Newbold* (1881) 17 Ch D 301
Cox v. *Riley* (1986)83 Cr. App.R.54
Dimmock v. *Hallett* (1866) LR 2 Ch App 21
DPP v. *Bignall* [1998] 1 Cr. App. R. 1
DPP v. *Lennon* [2006] EWHC 1201 (Admin)
H.L. Bolton (Engineering) Co. Ltd. v. *P.J. Graham & Sons Ltd*. [1957] 1 Q.B. 159
Keates v. *Cadogan* (1851) 10 CB 591
Leitch v. *Leydon* [1931] AC 90
Morphitis v. *Salmon* [1990] Crim. L.R. 48
R v. *Caldwell (James)* [1982] A.C. 341
R v. *Cunningham (Roy)* [1957] 2 Q.B. 396
R v. *G and another* [2004] 1 A.C. 1034
R v. *Whiteley (Nicholas Alan)* (1991)93 Cr. App. R. 25
Tesco Supermarkets Ltd v. *Nattrass* [1972] A.C. 153

American Judgements:

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)

Compuserve v. *Cyber Promotions* 962 F. Supp. 1015 (S.D. Ohio 1997)
eBay v. *Bidders Edge* 100 F. Supp. 2d 1058 (N.D. Cal. 2000)
Intel corp. v. *Hamidi* 114 Cal. Rptr. 2d 244 (2002) (first instance)
Intel corp. v. *Hamidi* 30 Cal. 4th 1342 (2003) (appeal)
Register.com, inc. v. *Verio, inc.* 126 F. Supp. 2d 238 (S.D.N.Y. 2000)
Sony v. *Universal Studios, Inc.*, 464 U.S. 417, 432 (1984)
Sotelo v. *DirectRevenue, LLC* 384 F.Supp.2d 1219 (N.D.Ill. 2005)
Thomas Kerrins v. *Intermix Media, Inc.* No. 2: 05-cv-05408-RGK-SS (C.D. Cal. Jan. 10, 2006)
Thrifty Tel v. *Bezeneck* 54 Cal. Rptr. 2d 468 (Cal. Ct. App. 1996)

Treaties/Statutes

English Legislation:

Computer Misuse Act 1990 (c. 18)
Police and Justice Act 2006 (c. 48)
Theft Act 1968 (c. 60)
Criminal Damage Act 1971 (c. 48)
Copyright Designs and Patents Act 1988 (c. 48)
Torts (Interference with Goods) Act 1977 (c. 32)

European Legislation:

Directive 91/250/EEC on the legal protection of computer programs
Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society

American Legislation:

Restatement (second) of Torts
CAN-SPAM Act 2003 (15 U.S.C 7701 et seq)

Secondary Literature

Reports:

Working Paper no. 44, *"Codification of the Criminal Law, General Principles, Criminal Liability of Corporations"*, the Law Commission, 30th June 1972

Books:

Code v2, Lessig, L., Basic Books, 2006

Computer Crimes and Digital Investigation, Walden, I. OUP, 2007

Contract Law: Text, Cases, and Materials, McKendrick, E. OUP, 2003

A Dictionary of Law, Law, J. & Martin, E.A., OUP, 2009, accessed online at <http://www.oxfordreference.com>

Encyclopaedia Britannica, 2009, accessed online at <http://www.britannica.com>

Entertainment Industry Economics: A Guide for Financial Analysis, 7th ed., Vogel, H.L., Cambridge University Press, 2007

Markesinis & Deakin's Tort Law, 4th ed., Deakin, S. et al, OUP, 1999

Salmond & Heuston on the law of Torts, 21st ed., Heuston R.F.V. & Buckely R.A., Sweet and Maxwell, 1996

Winfield and Jolowicz on Tort, 16th ed., Rogers, W.V.H., Sweet and Maxwell, 2002

Articles

Adams, A. A. *"Introduction: Valid protection or abusive control?"* 2006, International Review of Law, Computers & Technology, 20:3, 233

Burke D *"The Trouble with Trespass"* 1999, available at Social Science Research Network Electronic Paper Collection: http://papers.ssrn.com/paper.taf?abstract_id=223513

Gutmann, P., *"A Cost Analysis of Windows Vista Content Protection"*, last updated 2007, available at <http://www.cs.auckland.ac.nz/~pgut001/pubs/vista_cost.html>

Kerr, O.S., *"Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes"*, NYU Law Review, Vol. 78, No. 5, pp. 1596-1668, November 2003

Klang, M., *"Spyware: paying for software with our privacy"*, 2003, International Review of Law, Computers & Technology, 17:3, 313

Loren, L.P., *"Technological Protections in Copyright Law: Is More Legal Protection Needed?"* 2002, International Review of Law, Computers & Technology, 16:2, 133

MacEwan, N., *"The Computer Misuse Act 1990: Lessons from its Past and Predictions for its Future"*, Crim. L.R. 2008, 12, 955-967

Reeves, H. S., *"Property in Cyberspace"*, 1996, 63 U.CHI. L. REV. 761

Scheier, B. *"Real Story of the Rogue Rootkit,"* 2005, available at: <http://www.wired.com/politics/security/commentary/securitymatters/2005/11/69601>

Wong M.W.S., *"Cyber-trespass and 'Unauthorized Access' as Legal Mechanisms of Access Control: Lessons from the US Experience"*, 2007, International Journal of Law and Information Technology, Vol. 15 No. 1, OUP