Neutral Citation Number: [2010] IEHC 377

THE HIGH COURT

COMMERCIAL

2009 5472 P

BETWEEN

EMI RECORDS (IRELAND) LIMITED, SONY MUSIC ENTERTAINMENT IRELAND LIMITED, UNIVERSAL MUSIC IRELAND LIMITED, WARNER MUSIC IRELAND LIMITED AND WEA INTERNATIONAL INCORPORATED

PLAINTIFFS

AND

UPC COMMUNICATIONS IRELAND LIMITED

DEFENDANT

JUDGMENT of Mr. Justice Charleton delivered on the 11th day of October, 2010

1. The plaintiffs, who I will call the recording companies, record and release music and video for sale. They seek injunctions against the defendant, an internet service provider, to prevent the theft of their copyright by third parties illegally downloading it over the internet. The form of injunction sought is left to the discretion of the court. Hence, I will analyse various technical solutions.

2. Those enthused by music and video may legally buy it in a disc format or download it on the internet for a fee. Prices vary, but music in CD format or film captured on DVD can typically cost between €10 and €20 in a shop. A CD will contain up to 80 minutes of music, perhaps 15 tracks, and a DVD can store a 180 minute film. This case is about music. Both music and films are widely available for purchase to one's home computer over the internet. Because the material is in digital format, in the form of downloadable files, the quality is the same as that on a disc. To download a music track from the internet typically costs under €1 per music track but films are more expensive. All of these digital files are of original creative work. They are, as a matter of law, protected by copyright. Increasingly, as the evidence in this case has demonstrated, such protection has been undermined to the status of an empty formula. The recording companies complain that their entire business has been decimated by piracy on the internet. They claim that a whole generation is growing up, who instead of purchasing recordings in hard format or by legal download, simply access the sites on the internet that enable them to download for free the millions of music tracks that are available illegally worldwide.

3. The defendant, who I will call UPC, sells internet service to about 15% of the Irish market. Its turnover is in the order of €250M per year and the underlying nature of the business is profitable. It employs 800 staff. In its interface with customers it deals with about 35,000 inbound calls per month, of which it answers about 90%. Later in this judgment, I will refer in detail to the fact that a substantial portion of its 150,000 customers, or the children in their teenage and twenties years of these customers, are using the internet service provided by UPC to steal copyright material which is the property of the recording companies. UPC, as the internet service provider, transmits, in digital form, this copyright protected music through its system and into, and out of, the home personal computers that are used for copyright piracy. UPC claims it has no liability in respect of this activity because it is merely a conduit. The recording companies disagree.

4. The recording companies say they are entitled to an injunctive order of the Court requiring UPC to stop this infringing activity from taking place over its network. The recording companies say that UPC is in the best position to do this. The record companies have communicated with UPC not only as to the nature of the problem, but by actually giving it details whereby the infringers of copyright were detected, by the unique IP numbers assigned to their computers, illegally downloading their songs; but that they have been ignored. The recording companies claim that UPC is turning its face aside from this problem while maintaining a front of righteousness by having in place a customer use policy that condemns internet piracy but which it ignores deliberately in order increase its profit. The customer use policy of UPC makes it very clear that the internet service of UPC cannot be used to steal copyright material. This is a matter of contract, and for a breach of this obligation by the customer, UPC can terminate the contract. It never does. It is not so inclined.

5. At the end of their amended statement of claim, the recording companies are specific only to this extent as to what they seek:-

> "1. An injunction, pursuant to s. 37 and s. 40(4) of the Copyright and Related Rights Act, 2000, restraining the defendant internet service provider from infringing the copyright in sound recordings owned by, or exclusively licensed to, the plaintiffs by making available to the public copies of those sound recording without the plaintiffs' consent using its internet service facilities.
>
> 2. Without prejudice to the generality of the foregoing order, an order pursuant to s. 40(4) of the Copyright and Related Rights Act, 2000 that the defendant block or otherwise disable access by its subscribers to the website thePirateBay.org and related domain names, IP addresses and URL's, as set out in the schedule hereto attached, together with such other domain names, IP addresses and URL's as may reasonably be notified as related domain names by the plaintiffs' to the defendant from time to time."

6. Preferably, the recording companies seek a three strike solution: they would monitor the internet for infringements, inform UPC who then would be required on each occasion of breach of copyright to warn the infringer, up to three times, and then to discontinue service. In the alternative, blocking and diversion equipment is sought to be imposed on UPC by court order. These alternatives are later described in detail.

7. In defending this claim, UPC state that there is no liability in law for acting as a mere conduit for copyright infringement, and that it neither initiated the communication involved in piracy, chose the recipient, altered the information nor condoned the activity. In other

words, sections 37, permitting an injunction, and 40(4) of the Copyright and Related Rights Act 2000 ("the Act"), defining liability, do not apply to UPC at all. Even if the legislation mandates an injunction, UPC argues that no injunction should be granted because it would not be just or convenient; specifically that such an injunction would infringe the fundamental rights of internet users as to their privacy, as guaranteed by the European Convention on Human Rights and Fundamental Freedoms, would not be in accordance with the fundamental principles of European law, most particularly, proportionality and that the court would be drawn into the supervision of its own order.

The Nature of the Problem

8. I am satisfied that the business of the recording companies is being devastated by internet piracy. This not only undermines their business but ruins the ability of a generation of creative people in Ireland, and elsewhere, to establish a viable living. It is destructive of an important native industry. While the evidence focussed on the recording industry, the retail sector must also be affected by this wholesale theft. Furthermore, the evidence presented convinces me that a substantial portion of the generation now in their teenage years and twenties are actively dissuaded by illegal alternatives from legitimately purchasing music.

9. Some telling figures were produced during the course of evidence. Helen Sheehy, the solicitor on behalf of the plaintiffs, initiated three actions against Eircom plc, another internet service provider, with a view to discovering the names of infringers. I will shortly examine that action in detail. For the moment, suffice it to say that the recording companies had used DtecNet, a detection programme described later in this judgment, to uncover the IP addresses of individuals who were persistently infringing their copyright. Only the internet service providers know what IP address was ascribed to what customer on what particular day. In 2005, Ms. Sheehy applied for orders from the High Court so that seventeen individuals who were customers of Eircom, an internet service provider, would be named. In January, 2006 an order was sought in respect of a further forty-nine individuals. Then in June, 2007 a further twenty-three names and addresses were sought. All these three sets of orders were granted. Of the first seventeen individuals, the largest single uploader had 3,078 music files pirated, while the average was 628 files. The numbers increased with the second application. On the third application, the highest single infringer had 37,511 files while the average infringer had taken 8,400 files. It is reasonable to infer, from these figures alone, that even over the short period of two years involved that the problem of piracy through the internet was increasing rapidly.

10. Mr. Dick Doyle, Director General of the Irish Recorded Music Association ("IRMA") gave evidence which substantially supports the proposition that piracy of recorded music is a severe economic problem. Whereas the recording companies were aware of the issue of illegal downloading through the internet at the time of the enactment of the Copyright and Related Rights Act 2000, which was passed on the 10th July of that year and came into force on the 1st January of the following year, the problem was not then substantial. It is apparent from the action taken by the recording companies, to which I have just referred, from 2005 to 2007, that at an earlier date they had become alarmed by internet policy. Section 40(4) of the Act was first invoked by the recording companies against Eircom plc in aid of seeking some form of injunction against an internet service provider, which required them to block copyright theft, by the issuing of a plenary summons in 2008. Eircom is the largest internet service provider, with over 40% of the national market. I am satisfied that this was the logical place to start. In January 2009, the action against Eircom settled in the course of the hearing before this Court when they agreed to act in cooperation month-by-month on the detection of internet piracy by the recording companies, first warning their customers twice that what they were doing was illegal, and then shutting them off from internet access on a third infringement. Eircom has, as does UPC, an acceptable usage contract with its customers mandating termination for illegal internet use. Eircom takes its customer contract seriously. UPC, as will emerge later, does not unless it can profit from it. In settling the case with Eircom, the recording companies agreed to bring proceedings against the other internet service providers but, as Mr. Doyle told me, and I accept, they would probably have done so anyway.

11. Between 2005 and 2009 the recording companies experienced a reduction of 40% in the Irish market for the legal sale of recorded music. This is equivalent to €64 million in sales. Up to August, 2008 the country was experiencing a decade of growing and heavy consumer spending. The figure is probably, therefore, an underestimate. Mr. Doyle suggests that a large proportion of that decline was due to illegal downloading. Fairly, he states that it is impossible to say that every single illegal download resulted in the loss of a sale, because what is free is often just taken, and perhaps never listened to. The figures produced by Mr. Doyle indicate that the relevant surveys show a loss of between 20% and 30% as a proportion of decline in sales to what is illegally downloaded. In referring to the relevant research, Mr. Doyle posited at about 1:0.42 as to the ratio of unauthorised downloaders per broadband internet line. There are 1,571,000 broadband subscribers in Ireland of which, if the international studies translate, some 675,000 people are likely to be engaged in some form of illegal downloading from time to time. I am satisfied these studies are accurate and apply to Ireland. The average number of files illegally downloaded per month for each of these individuals, international research suggests, was 20.2. The evidence posits the probability that there are around 163.7 million illegally downloaded songs sitting on computers in Ireland waiting for people here, or in other parts of the world, to, in turn, download these songs from them. This represents a loss to the music industry which, if measured at 99c per illegal download speaks for itself. Mr. Doyle posited that the lower 20% ratio might be applied whereby at least €20m in lost sales are being caused to the Irish market by illegal downloads on an annual basis. Similar losses in revenue must also undermine revenue to record shops.

12. The nature of this problem was further described by Willie Kavanagh, the Chairman of EMI Records (Ireland) Limited. His evidence was that the mass illegal availability of sound recordings, made available without authorisation or payment through the internet, has done untold damage to the development of the legitimate music industry and has caused major damage to traditional CD sales and to legal internet sales. While Mr. Kavanagh fairly admitted that CD sales were likely to decline anyway, as legitimate downloads became available on the internet, and that these had increased from a zero base and continued to grow, the views expressed by Mr. Doyle, he said, were well accepted across the industry as to the nature of the decline and the reason for it.

13. Illegal downloading is done with considerable ease. Mr. Kavanagh conducted an exercise, which in his case was legal because he works for the company which holds the copyright, whereby he attempted to illegally download the track "Viva la Vida", a track produced by the group Coldplay. He went to a well-known site for facilitating music piracy called 'The Pirate Bay'. First, he installed on his computer at home a peer-to-peer file sharing application called LimeWire. This took a few seconds. This was free and was enabled very swiftly after he became a member of the Gnutella/LimeWire peer-to-peer network. Then, using the relevant software and the same website, he did a search on the internet for the track. A huge number of hosts for the track came up and he downloaded the song onto his computer in a very short time. At one stage in the process a notice appeared as asking him to "respect copyright". This, he correctly described, tactfully, as a form of hypocrisy. In less than three minutes he had joined the relevant website, downloaded the necessary software, accessed the relevant swarms of computers offering the track illegally, and downloaded the targeted song. Once this is done once, it is quicker the next time and a person is likely to steal again. His written witness statement gives other examples. He also recalled, in evidence, looking for the film "Batman-The Dark Knight", before it was released in the cinemas and being able to get it illegally, for no payment, on the internet. If the pirated version is filmed covertly in a cinema, it is likely to be of poor quality; once the DVD is available in shops, or perhaps by other means prior to that event, the internet will be full of perfect digital reproductions. The particular track "Viva la Vida" was offered as an example of the losses that the recording companies suffer, and through them, those who have the strongest moral right to copyright, that is the creative artists behind music.

The album from which "Viva la Vida" was taken cost around €1 million to make and €10 million to market.

14. This scourge of internet piracy strongly affects Irish musicians, most of whom pay tax in Ireland. 'Aslan' is a distinguished Irish group which has a loyal fan base; but not all of them believe in paying for music. Previous sales of their albums were excellent, about 35,000 per album, and in respect of one called "Platinum Collection", a three CD box set, 50,000 copies were sold. More recently, an album called "Uncased" was released and only 6,000 copies were sold. Perhaps, it might be thought, the album was not popular and did not sell well? In contrast, a search was made to see how many illegal downloads had been made on the internet from that album, and 22,000 were traced.

15. The implications of this are that those involved in creative work will get a substantially, and unfairly, reduced return for the expenditure of their talent in creative work. From the point of view of the recording companies, if there are no profits, and no royalties to artists, the legal sale of recorded music, through the preparation of albums, will cease. As Mr. Kavanagh put it: "If you don't get a return on an investment and you go down the same road again and invest the same money again and expect a different outcome, the likelihood is we would be reluctant to invest in another album".

16. The relevant evidence and surveys presented to the Court by Mr. Kavanagh and Mr. Doyle indicates that with the growth of broadband internet rollout, the easy and unimpeded piracy of music will grow. The Court sees no reason why a person, who is not habituated to purchasing recorded music, would not take it for free over the internet. I think that Ireland is broadly comparable to Australia in respect of our internet usage habits. The evidence convinces me that if we are not now at the stage, we are moving towards the situation where teenagers and students have, or will have, an average of many hundreds of illegally copied songs on each of their digital music players. The Australian survey referred to in evidence probably represents the present situation in Ireland; and the even bleaker future for the music industry. As between those who are under 20, and over 25, the proportion of tracks not paid for is likely to be over 60% in the first category, and under 15% for the older category. Time is moving on and more and more young people are embracing internet music piracy. When Mr. Kavanagh told me that he had no reason to believe anything that contradicted this survey, I noted that it might be challenged in cross-examination or rebutted by contrary evidence. This did not happen. Further, another careful international survey indicated that between 49% and 83% of all internet traffic, with a night time peak of 95%, is accounted for by peer-to-peer communications. The time when the internet is most used in this way is at night time. Significantly, UPC shapes its internet traffic so that peer-to-peer and other forms of communication are competing for internet use during business hours, when teenagers and students are less at home, but peer-to-peer downloading and uploading is throttled to around a third during the evening and night.

17. I have carefully observed the evidence given by Ms Sheehy, Mr. Doyle and Mr. Kavanagh. From the point of view of consistency of narrative, demeanour and internal cohesion, I am satisfied to rely on all of their evidence.

Economic Issues

18. The evidence establishes definitively that copyright is being infringed on the UPC network. I do not accept any of the evidence from UPC as to its unawareness of this process. Nor do I accept that it has not thought about this issue and considered whether it is making a profit from it.

19. More widely, however, internet piracy is an economic and a moral problem. Were men to walk into a cinema and in the dark, set up a small tripod for a machine to digitally record the latest movie blockbuster, to use the appropriate colloquial terminology, most right thinking people would be appalled. To entertain themselves and their families at home, they would have to wait three or four months to buy the DVD on its release and spend about €15 to have the film and whatever extras were added on to make it attractive. It is hardly credible that cinema owners would not be aware of this problem taking place. If they did nothing, and allowed people to proceed with illegally capturing the film, the first step would have been taken with their acquiescence in the undermining of copyright. Attendance at the film would plummet, because a group of friends would be drawn into deciding that a cheaper alternative for say five or ten of them, instead of having to spend between €50 and €100 on cinema admission, would be to buy a pirated copy of the film and watch it in the comfort of their home on the now almost ubiquitous flat screen television of large size that graces our home life. If nothing were done about the men, their camera and their tripod, their digital reproduction equipment and their sales, on the release of the DVD of the film, legal purchases would be minimal. Similarly, in the week of commencing writing this, the National Youth Orchestra of Ireland presented a stirring new composition, 'Summer Overture' by Shaun Davey, in the National Concert Hall. . Nowadays it is possible to attend a concert and to have CDs of it legally for sale fifteen minutes after conclusion. A person could covertly capture the music on a small digital recorder. If that individual went out to a van in which he had a great deal of digital copying equipment, reproduced it without permission and sold the CDs to those leaving the concert, it would rightly be regarded as flagrant abuse of copyright. I cannot see how an illegal recording on site and the subsequent public or internet offering for free, with no return to the composer or performer for their creativity, is anything other than a scandal. I have no doubt that any responsible cinema owner, or concert hall owner would stop internet piracy, if made aware of it. I am further satisfied that a reasonable person in that position would be vigilant to prevent it in a cinema or in a concert venue. A failure to address those problems, by those who can address the abuse, is not excusable. It constitutes the abuse of the economic interests of the creative community. This kind of theft is shameful. Many who see that activity on the street would shun the commerce of exploiting the rights of artists for no return. Peer pressure would prevent much of it. But the internet allows a dispensation from shame, as internet thieves figure that no one will know what is being done behind the closed doors of internet access. Essentially, that coupled with the failure of internet service providers to act like a responsible cinema or concert venue owner would act, is why the problem is so extreme

20. There is no difference between the public situations I have described and the piracy of music tracks over the internet. It has the same consequence. The conduit for that illegal activity is, however, not the street or the pavement outside a cinema; it is the internet service providers. It is clear that they have an economic and moral obligation to address the problem. I do not accept any of the evidence from UPC, referred to later in this judgment, as to why this has not been done. Instead, the effect on the market place of illegal downloads, through the internet, is to increase the profit levels of internet service providers. Relevant correspondence from within UPC is profoundly disturbing as to the reality of their approach.

21. The evidence establishes that this problem is a massive one. This is an instance where the multiplication on a huge scale of small problems has changed the nature of the issue into a huge pilfering of the resources of creative artists. For each individual person, the number of downloads cannot be regarded as being on a commercial scale. It is the multiplication of the problem through millions of individuals feeling free to use the internet to pirate the copyright of creative artists and recording companies that has created the undermining of that right on a foundational scale.

22. I now need to describe the nature of internet communications in detail, for it is on this detail that the legal authority of the court to grant injunctive relief is circumscribed. In that regard, the nature of the potential solutions to the issue of internet piracy must also be addressed. The interaction of the parties requires also to be examined. The relevant legislation is then analysed.

Internet Access
23. The internet consists of millions of linked computers. The principal points of linkage are internet service providers, of which UPC is one. Those who subscribed to broadband access are provided with a cable modem that gives an Ethernet connection. Many of UPC's customers subscribe for voice telephony, television and internet access over this connection. Through a wireless router, internet service can be used within the range of the wireless router, provided the appropriate customer identification number, supplied by UPC to the customer, is keyed into the computer. For UPC, the cable modem is identified and authorized through a MAC address. This is registered in UPC to a particular customer at a particular place and also records the kind of service to be paid for and the level of service for internet broadband access that is allowable in accordance with the fee paid. The separate IP address is assigned from day to day by UPC, as internet service provider. They alone know the identity of the customer using that IP address at any particular time. Because there are millions of IP addresses, no one apart from UPC, merely having the IP address that was used to infringe copyright can discover the identity of infringing subscribers. Anyone can find out the banks millions of numbers assigned to particular internet service providers; but that is all that can be learned.

24. When the cable modem of a UPC connected computer boots up, UPC will verify that the MAC address is assigned to the correct cable modem, it will allocate a temporary IP address for the boot process, it will check on the profile of the service subscribed for in accordance with what the customer has paid for, it will then access the internet and the customer can proceed. The customer will have contracted to use the service in accordance with the Acceptable Usage Policy of UPC. The boot up process includes the collection of log information that records the IP addresses allocated to the customer's equipment, identified by the MAC address, and the relevant time.

25. UPC employs sophisticated monitoring and management tools. In particular, the bandwidth usage of the customer is monitored. Traffic monitoring, classification, and the enforcement of acceptable usage, is done through Cisco SCE8000 Systems. This performs a classification of the total aggregated traffic.

26. The use which a customer makes of their broadband facility is reported on through the ServAssure Programme that is run at the end of every month. This data refers to MAC addresses, because there is no need to refer to IP addresses in this context, since the MAC address is not movable for this purpose. UPC then manually cross references that data with the customer database whereby account details are determined and checked. The data is then cross referenced to another manual database to determine whether or not the account holder has had previous warnings on an excess use of bandwidth beyond what they have paid for. Following this exercise the account holder, if using excessive bandwidth, will receive either a first or second warning. In practice, as I understand it, once a warning is given, and bandwidth usage does not cease, the customer is billed up a level to the next highest, or above, bandwidth payment structure. The Acceptable Usage Policy, which I will turn to shortly, allows customers to be cut off for using excessive bandwidth. However, I understand from the evidence of Anna Coyle, who is in charge of billing within UPC, that the current policy is to retain valuable customers and to persuade them to move up to a higher bandwidth and pay more money. This is done by warning them and then just billing them at the higher bandwidth. People are not cut off in respect of this, there are simply sent a higher bill. To some extent the evidence is confusing as to whether one or two warnings are given, depending upon the package that the customer has contracted for. The evidence is clear, however, that UPC pursue a policy of retaining customers and requiring them to pay more by reference to the Acceptable Usage Policy whereby if they use more than they have contracted for, they are required to pay in accordance with the level billed. Those who do not pay are cut off. There is no negotiation on this issue.

27. Traffic monitoring, through deep packet inspection, is used by UPC to shape traffic. The current policy is based on a general shaping of peer-to-peer traffic. This uses different levels for upstream and downstream. The shaping is applied to the total aggregated traffic and is not targeted at any individual user. The thresholds are statistically defined and can be changed through input. This shaping is applied to peer-to-peer traffic, to reduce its potential for domination of the network, during peak hours for computer usage which are daily from 17.00 to 24.00. In off peak hours, which coincide in part with business hours, no shaping occurs.

28. The nature of peer-to-peer traffic has been described in evidence in technical terms. I wish to give a brief description here. Professor Paddy Nixon, of University College Dublin, told me that the relevant studies showed an analysis of internet traffic that was 70% peer-to-peer in Eastern Europe and 56% in Western Europe. As to encrypted peer-to-peer traffic, while some reports put that level as well over 25%, the studies referred to in evidence showed it at 20% or just under. Peer-to-peer networks are established using appropriate technologies, such as BitTorrent, whereby each participant becomes both a downloader of material and an uploader. The principles applied in legal peer-to-peer file sharing and illegal peer-to-peer file sharing are the same. A lengthy musical, or other, work would be split up into thousands of digital parcels, each one of which carries an identifying code which indicates that it is a particular track. This can be checked by anyone over the internet through DtecNet whereby identification can be made to the particular IP address that is engaged in the process of uploading/downloading copyright material without permission. Whereas a suggestion was made by counsel during the course of the case, that these file # numbers degrade over time that was not backed up by any evidence. A participant, having downloaded the relevant software for free over the internet, such as eDonkey, or Gnutella, will find out on a site where a particular track is available and then join his computer, through the internet service provider, to a swarm of computers worldwide that has the material available for illegal downloading. Each user will open a file on their computer for this sharing purpose. What they already have is shared, potentially, with every other computer in a swarm, while what every other computer in the swarm has on their corresponding file, is potentially shared with the illegal downloader. What makes peer-to-peer communication useful, in terms of legal applications, is that it markedly increases the swiftness of a download and that the party from whom the download is taking place, does not require the same level of power as if the traffic were all coming from one source. Because the traffic is taken from hundreds or thousands of computers, there are that number of platforms, and their combined power, for hosting the information and for transmitting it through the network to the person who wants the download. Each piece, marked with the relevant # file, is also identified digitally as to the place in which it should sit in the overall work. The computer identifies these pieces and places them in an appropriate order. Thus, instead of the scale of A major arriving as A, C#, E, D, B etc, it will arrive A, B, C#, D, E by reference to the identifying codes. A may arrive from a computer in Kerry, and E may arrive from a computer in Germany, but they will all be assembled on the users computer in the right order so that perfect digital reproduction of the original is attained. This is usually, whether it is illegal or legal, then downloaded onto an iPod, or other portable device. Whereas the computer in Kerry, and the computer in Germany, are outside the UPC network, and may be transmitted from and through several different internet service providers, for the copy to arrive at a UPC broadband subscriber's computer, it must pass through the UPC network that is the subject matter of this case. For seconds, or for minutes, in digital form, it is on that network before it arrives, unless blocked or diverted, at a UPC subscriber's computer. During the course of transmission there may be momentary stopping and starting, but the pieces will be sent out in the right order.

Legal and Illegal Peer-to-Peer
29. I am not convinced by the evidence, in particular that of Professor Nixon, that any solution based on blocking all peer-to-peer traffic, or severely constricting it, is reasonable. I am convinced by his evidence that the volume of peer-to-peer usage on the internet will grow. As legitimate downloads are offered on the internet, it strongly favors this lawful activity that peer-to-peer technologies can be used. For instance, in downloading a sound recording from the RTÉ website, or a film from the BBC website, the

application of peer-to-peer technology means that the host can rely on the person desiring the film joining a swarm of computers that have it available, whereby the power of the server can be less, thus reducing costs, because the download/upload procedure is relying on the connection of many hundreds or thousands of computers that have the work available for sharing already. Storage facilities such as the S3 service offered by Amazon, allow companies or organisations in diverse locations to download data by reference not only to the central computer, from which the service is offered, but by the branch networks being online, having the data on file, and sharing it through peer-to-peer technology. This is likely to be a growing part of legitimate activity. In addition, there are some sites, at present small, of which an example is the LimeWire Store, which offer legal downloads using peer-to-peer technology. That is likely to grow as well.

30. What I am also satisfied of is that the large majority of the current use of peer-to-peer technology is for the purpose of illegally downloading copyright material. In that regard, I take into account the view expressed by Professor Nixon that the illegal use of peer-to-peer was in a majority; the eventual concession by Anna Coyle and the evidence of Dick Doyle. The studies attached to the relevant witness statements and admitted to evidence by consent bear this out. What cannot be predicted, however, is the level of growth of legal peer-to-peer file sharing and whether lawful use will eventually become the majority. While this technology is certainly used at the present time to account for a large majority of internet piracy of copyright material, trends in the future may mean that it is in a minority.

31. Even if that were not so, it would not be in accordance with the principle of proportionality to use a blunt instrument for the deterrence, or rendering impossible, of illegal activity, when the effect of that would inevitably lead to the infringement on the right of communication through the internet.

32. Another solution proposed, by way of injunctive relief, was to search out the platforms most often used within peer-to-peer sharing protocols for illegal file sharing, to identify them by deep packet inspection, and to severely throttle or block these communications. There are two reasons why this also is not proportionate. Firstly, the relevant software may be designed to use a number of applications. Those involved in copyright piracy, would readily, and swiftly, release new applications for downloads. Illegal users would switch to them readily. Secondly, there is no satisfactory evidence upon which I can rely which indicates to me that a list of protocols, such as eDonkey, gNnutella and LimeWire, are not also used legally. To block these communications would not be proportional. It might have the effect of cutting off a certain amount of illegal peer-to-peer file sharing, but it would also have an effect on the ability of internet users to lawfully communicate with each other.

33. I would reject any solution that is based on any substantial constriction in the communication of material lawfully available on the internet unless the harm is demonstrated to be so grave as to illegal file sharing of copyright material as to render that both necessary and just. It is not so demonstrated, especially as there are viable alternatives. I now consider each of the potential technological responses to internet piracy of copyright that has been described in the evidence in order to supply the detail for these conclusions.

Solution I: Detection

34. The IP address of those engaging in the peer-to-peer uploading/downloading of copyright material can be discovered easily and accurately. DtecNet software is a process which was described in evidence by Thomas Sehested. In essence, by checking with Résaux IP Européens ("RIPE"), an organisation based in Paris, a list of IP addresses provided to internet service providers in Europe is obtained. Digital files of copyright material are then obtained from the owners. There may be several thousand of these obtained directly from the record companies. As the download is proceeding through the system it carries the IP address of those who are downloading material. DtecNet does what any user of a peer-to-peer network does in order to obtain a download. No extra information is obtained. The fact of the download together with IP address, the digital information identifying the copyright material and the time or the crucial data is obtained. DtecNet searches peer-to-peer networks for files being uploaded which are subject to copyright. On finding such a file, DtecNet requests the file. This is then transmitted to, and copied, by DtecNet's computer. It is integral to this process that basic information about the uploader from whom the work is being transmitted is obtained. The examples produced in Court show that the user's pseudonym and the IP address of the user appears together with the relevant time, date and identification of the copyright material. As part of this process, if the IP address was registered to an Irish internet service provider, DtecNet identified how many sound recordings were being made available by that user on peer-to-peer software. A list of the files was then captured in the form of a log containing the name, size and hash value of user's shared files. Although a music file may be split up in several hundred pieces, each of them carries a sufficient identification through the file # for it to be fitted into an appropriate order of sense and sufficient to clearly identify that it is a portion of a work which is subject to copyright. In all of the examples of which the Court was provided evidence, there is nothing to suggest that if only a tiny portion of the work was being uploaded that that would be insufficient to identify it. Rather, what peer-to-peer involves is obtaining the entire music recording that is desired. The file # identifier ensures that it is put into a correct format and order. The process of DtecNet is automatic, in the sense that the handshake between the computers, in peer-to-peer terminology, is fully automated. The search for particular files, for example the 1,000 most popular songs relevant to the recording companies, at that time, is inputted for the purpose of search. I am satisfied that from the evidence that the process is highly accurate. The activity log further transcribes the activity whereby the evidence is secured in a reliable format. There was nothing in the evidence to suggest to me that this process was subject to any degree of substantial error. Furthermore, the evidence establishes that there is a substantial problem on the UPC network with copyright piracy. Various figures on a monthly or annual basis were produced in Court. These related to an estimate of 15,000 per month, on a test run by DtecNet on 350 random tracks from a list of 10,000 U.K., Irish and internationally popular tracks. An extrapolation was made that at their peak downloads were likely to reach around 47,000 per month. These, however, are individual incidents. A person may be downloading a number of tracks in a single sitting, as it were, at their computer. A person may go back and download on their computer a number of times in the day. They may leave their computer on all day, downloading continually. It is highly unlikely that a person who enjoys an experience, having done it once, will simply desist. The figures produced by Ms. Sheehy speak for themselves. If, therefore, one is responding on a month-by-month basis, while it is difficult to say how many individual infringers one may be dealing with, it is certainly a small fraction of 47,500. Returning again to the figures mentioned by Ms. Sheehy on previous tests, it is apparent that there are likely to be, at most, some few thousand of them. Of them, perhaps a hundred or so will be the leaders in culpability. These few people are the ones who need to be processed. It is also apparent that the recording companies are going to have to make a choice in the implementation of any injunctive relief which they are seeking, whereby the worst infringers, namely those who download most frequently or who have the most illegally copied material on offer, will be prioritised

35. There are two potential methods of evading the DtecNet process. The first is by the use of proxy IP addresses. A sophisticated computer technician could hack into another person's computer, and then request files using peer-to-peer technology. They would be downloaded to the second computer via peer-to-peer technology and, as I understand, then directly download it, bypassing peer-to-peer communications, and therefore DtecNet, back to the original computer user. A second way would involve using another computer as a proxy server. There are some free sites, as I understand the evidence, offering this service. There are, in addition, ways of paying for the hire of another computer so that this process can be engaged in. The figures that I have obtained from Mr. Sehested in evidence indicate to me that the current use of this technology to avoid the ultimate IP address that the user resides on is now

around 0.3%. With any solution, there will be a technology battle, whereby this problem may increase, and may need to be addressed. As of the current time I do not regard it as significant.

36. Secondly, peer-to-peer downloaders can use encryption. This is not a problem. An encrypted communication is only of use if the party sending it knows that the party receiving it can decode the message. This is how Mr. Sehested put the matter:-

> "P2P encryptions basically make it hard… it encrypts the actual traffic flowing in and out of the network, but as we are residing within the network, actually communicating with the users on equal terms, encryption will not affect our scanning. However, if you were do what is called a "de-pack inspection", that basically means if you are looking at the packages that is flowing back and forth, then encryption would hide that traffic so you are not able to see that it is potentially P2P traffic. But as we are actually residing on… either end of the communication, the traffic being encrypted is not an issue for our monitoring… [b]ecause we are essentially part of the network, so we could also communicate encrypted. So the idea of encryption is that if you have two endpoints, if anybody is standing in the middle of that, they won't be able to intercept that traffic, it will be encrypted to them. But if you are either end of the spectrum, you will have a key to unencrypt it, and we are on that side of it."

37. Further, as I understand it, those internet thieves using peer-to-peer encryption, download standardised forms of encryption so that mass communication can take place. I do not regard this as a substantial reason why the use of DtecNet technology would not be appropriate. The analysis thus supports the conclusion that I have reached that the detection, notification and termination solution is viable and proportionate.

Solution II: Global File Registry

38. The solution of detection and diversion that was described in evidence by Jorg Michael Speck involves several steps: this is called Global File Registry. A programme which is capable of being integrated into the Cisco 8000 of the Firmwear upgrade requires, firstly, the identification of files which are not either out of copyright, by reason of a lapse of time, or in respect of which copyright has been waived. In this regard, the relevant programme has a database of around four million tracks which are subject to copyright. Secondly, an alternative offering of around one million tracks is made available for legal download through this system. Global File Registry can operate on a mirrored form of network, whereby there is no encumbrance of the speed or efficiency of the internet service provider's offering to its customers. The database of music tracks which are likely to be infringed is taken from the owners. In microseconds, any peer-to-peer transmission involving the illicit sharing of copyright material is identified through the file hash. This indicates the contents and mandates the programme to take action. Once the file hash is cross-referenced to copyright material, the sought for file-link by the customer of the internet service provider is immediately terminated. Then, the second aspect of the system occurs. The customer seeking a particular track unlawfully is immediately diverted to a site, made available through Global File Registry, where that track may be accessed legally. The system uses deep packet inspection. Legal traffic is never interrupted. Privacy is not infringed as the system simply reads numbers which identify the illicit nature of the transmission. Integral to that, I infer from the other evidence presented to the Court, is that a relevant computer address can also be recovered, as it is part of the transmission. There are, therefore, no privacy issues involved as no aspect of the system described involves the identification of a customer. Therefore, the firewall which exists between the allocation of a bank of IP numbers through RIPE, which is publicly available, and the day-to-day, or hour-to-hour, ascription of that number by an internet service provider to a particular customer, is never breached. The recording companies can never, through Global File Registry, or any other system, discover who it is that is infringing their copyright materials. Only the internet service provider on being notified of an infringement through DtecNet can find that out.

39. Global File Registry by-passes any response by way of detection, notification, education and termination in favour of immediate interruptions. The advantage of the system is that it offers a legitimate alternative which Mr. Speck described as offering "solid value". This changes the passive transmission of internet service provider customer's data into intervention. It can operate as a source of revenue to the internet service provider since arrangements are predicated to be made between the companies offering internet service and the recording companies. Thus, the attempt to illicitly download a music track by peer-to-peer file sharing is immediately interrupted and a diversion is effected to a site, shared by the internet service provider and the music industry, whereby a legal download may be made by payment through a credit card or by an addition to a customer's bill from its internet service provider.

40. A similar system is operated by police in Australia in relation to about 70,000 child pornography images. These are identified by reference to the file hash, but in that instance the transmission is simply interrupted. I would imagine that this system, which is fully tested and in operation, also involves the gathering of data as to the user for criminal detection purposes, but this was not developed in evidence. That police agenda does not form part of the operation for the disablement of copyright theft.

41. While the system is now partnered with the Cisco Corporation as a joint venture, and while it presents as a viable future alternative, it is yet to be fully tested. It would not be right for the Court to order such a system by way of injunctive relief because its integration and testing will take time. A trial exists with an Australian internet service provider but this trial, the Court notes, is only in respect of 200 musical tracks. To ramp up the trial towards a significant number of tracks, which in an Irish context would certainly run into several thousand, involves moving into an area which is not sufficiently predictable. It is possible, as was established in cross-examination, for persistence to lead a determined customer to an illegal download. It is also possible that the file hash in a very popular music track, that was constantly blocked, could be changed. I am satisfied that this would be an elaborate process. There would be a likely response from the music industry whereby, that would be detected and added, under that new format, to the files to be searched for and detected in the course of illegal transmission.

42. There are obvious advantages to the Global File Registry system. The routes around it are difficult and time consuming. It represents a viable future way of responding to internet copyright piracy. It has no privacy implications. Any aspect of encoding is not demonstrated in the evidence to be different to the obvious solution of uploading the encryption programmes that are widely shared in this mass market. However, this system requires further work in order to operate at the level required. Finally, on this issue, I am not satisfied that in order to markedly decrease the internet piracy of copyright material that it is necessary to upload the entire discography of modern civilisation. Instead, the evidence demonstrates that deterring, through interruption and diversion, the most widely shared musical tracks at a particular time is highly effective. These need only be in the hundreds or thousands of tracks level. In the future, with development, the evidence establishes that this solution to internet piracy is likely to be effective.

Solution III: CopySense

43. In the United States, the Digital Millennium Copyright Act 2000 and the relevant legislation governing higher education institutions require all universities to control illegal file sharing on their networks. Charles Benjamin, the senior network and systems administrator for the Department of Housing and Residents in the University of Florida, gave evidence as to how the system functions in the University. This is called CopySense.

44. Every student who enters the University receives an email which informs them that they are to avoid the violation of copyright through peer-to-peer downloading. Despite this, many students in their first time regularly upload and download music which is subject to copyright. In response to this, the university has a graduated series of sanctions. The implementation of that graduated response is achieved by the use of the CopySense programme produced by Audible Magic. The University evaluated it as most appropriate for its needs because it had a database of six million signatures of copyright works, when it was first chosen, and now has increased that to some eight million tracks. Mr. Benjamin, in his witness statement described how it works:-

> "It operates like an anti-virus programme in a sense that there is a database of signatures, in the case of CopySense signatures of copyright media, frequently updated that is compared to data being transmitted on the network. It creates a violation notice which we use to place the student in a restricted [network], disrupting the P2P transmission and restricting internet access to the … campus. It does not monitor the contents of email, web travel, instant messaging, FDP, newsgroups, legal copyrights works being downloaded etc. It only monitors peer-to-peer protocol."

45. The system is not connected to the University of Florida network. Instead, the transmissions are mirrored under a parallel system and analysed. Once a violation is detected, the CopySense programme is mandated to interrupt the communication, immediately terminating it, and sending a warning notice to the students. The system does not cause any disruption of the network, because of the manner in which it is deployed. Instead, the network is made available for legitimate peer-to-peer activity.

46. The level at which this succeeds is less than with a medium size internet service provider, such as UCP, which has 150,000 customers. The university has 49,000 students, with 200 buildings in the Housing Department and with 10,000 Ethernet connections for the students that live in the university. The formal graduated response was described by Mr. Benjamin in this way:-

> "We then operate a system of giving warning notices to students who attempt to share copyright material, essentially it is a graduated response. Accordingly when a student is first detected sharing or downloading copyright material with a peer-to-peer programme, they are sent an email warning them of the violation and are directed to a web page. The web page contains the unique case number, the violation level, and the type of peer-to-peer protocol that was detected and a description of the [University Housing Unit] acceptable usage policies… The students must click "I will comply" before the restriction is lifted. In the first occasion the student is restricted to on campus usage for 30 minutes. If there is a second violation the student is restricted to on campus usage for five days and if there is a third violation, the student is directed to appear before the Housing Judicial Office. It is remarkably effective. We do not get a lot of repeat offenders, less than 2% proceed to level 3. Statistics show that the three graduated response system educates the student not to use P2P software in conjunction with copyrighted material. We have seen consistent results in each semester since the installation."

47. On the issue of privacy, the inspection maintained by CopySense on the appliance which mirrors the university network access to the internet does not violate privacy. The university is not looking at content. Instead, similar considerations apply as in the DtecNet solution. There are some instances where the university does monitor the content of communications, but this is not one of them. There are therefore no implications in respect of privacy.

48. The strong effectiveness of the CopySense solution within the University of Florida is dependent on the high levels of detection that the system displays, the discipline inherent within the university setting and the ultimate sanction of expulsion that may emerge for repeated violations. As I understand Mr. Benjamin, for a modern student to be denied internet access is to place them in a position where they would be left dependent on text books; many lectures are also offered or summarised online. In effect, this will leave the student without vital research resources and result in the termination of their relationship with the university. In consequence, the very good results can be explained by that, but only in part. While I accept that a student group is quite different from an outside internet service provider and its customers, it is also apparent that detection and warning have a salutary effect on those who seek to violate copyright. This solution does not undermine the effectiveness of the network. The first and second stages of the process are automated. Six dedicated staff and some part-timers manage the system. I am satisfied that this is not a severe burden as those employees also manage the telephone system and security monitoring for the housing network.

49. The system can be by-passed by the student returning home and, in the absence of similar general controls through internet service providers in the United States, violating copyright in a private setting. Nonetheless it is clear that the system is enormously effective, it does not impact on the network efficiency, is balanced in its approach by way of a graduated response and has no impact on privacy. To deploy the CopySense solution on an internet service provider, with 150,000 customers, would require testing an appropriate expansion of the system. While detection may not be 100% effective, I accept Mr. Benjamin's evidence that it captures the bulk of violations. Were there a willingness by UPC to engage with such a system, it could readily be made to work. It is clear why they do not wish to so engage.

The Attitude of UPC

50. I am not satisfied that the attitude of UPC toward the illegal sharing of copyright material over the internet is either reasonable or fair. I believe that the two witnesses who gave evidence on behalf of UPC, Anna Coyle and Conor Harrison, were intentionally placed by their employer in an impossible position. They are not the controlling minds behind UPC in Ireland. They do not set UPC policy. In the light of all the evidence, I accept what Dick Doyle, on behalf of the recording companies said in relation to the description as to its services offered by UPC in a magazine entitled "Fusion, Issue No. 3". This offers various broadbands speeds, under the titles of Fiber 5, Fiber 15 and Fiber 30. It is a dubious encouragement to purchase internet access. This is a domestic offering, it should be noted, not a commercial one. The offering is a commercial use of internet piracy and an encouragement of it. The following quote appears that describes the service:-

> "Fiber 15:
>
> A download speed of 15Mb is suitable for users who regularly download or send large files such as music or movies. This speed also supports online gamers and video calling, which is becoming more and more popular with our customers. An ideal pack for families."

51. The Court regards this, in accepting Mr Doyle's evidence as accurate, as the exploitation by UPC of the difficulties of the recording companies with piracy. On its own, this could be regarded as offering increased bandwidth for legal purposes, such as gaming. The correspondence does not support that view as a probability. This view is not taken in isolation, but is backed up by disturbing written evidence which the UPC witness could not be expected to explain satisfactorily. The Court's comments, in this regard, are not ascribed to these witnesses but to the defendant UPC, as an organization. In the context of the settlement of the Eircom case in January 2009, the marketing manager of UPC was sent an email on 29th January which stated:-

> "We should not link what we are doing in marketing (on automatic upgrades/disconnect) with illegal downloads. We want to distance ourselves from this debate for as long is possible."

Later on, there was another email within UPC at high management level:-

> "Understand, however even in the face of negative of backlash we should not say anything about what we think they may be using bandwidth capacity for. No mention to illegal downloads, rather focus should be you are exceeding your bandwidth capacity, therefore we are moving you up a tier or we are disconnecting you. There will be a lot of attention of this topic going forward. I would not want a situation whereby users on boards. ie on receipt of a letter/verbal feedback from us, write up that we are taking steps because we think they might be using capacity to do smth illegal. I would not want anything out there in the public domain that may give them an extra stick to beat us with us. This settlement would be more than enough ammunition for them. I wouldn't want to give them anything extra."

This was then followed by a reference to the UPC policy which, in summary may be quoted as follows as to the obligation which they impose upon their customers on providing internet service:-

> "As a general principal you must not use the services in any way that is unlawful or illegal or in any way that effects the enjoyment of other users of the services or the internet."

52. Specific provisions exist whereby UPC may terminate a customer's service for the infringement of copyright. They have never done this, nor do they have any interest in doing it. Specifically the UPC customer contract provides:-

> "Any images, photographs, articles, pages, designs, drawings, software, music, information and other materials published on the internet and the services are protected by copyright. Published material on the internet and on the services does not mean that it is available for anyone to copy. Unless the owner of that copyright specifically states that you may copy their work, you should assume that you cannot. It is an infringement of copyright to reproduce, adapt, translate, broadcast or perform copyright protected material without permission, to make infringing copies available to the public or otherwise to knowingly deal in infringing copies. The services must not be used, directly or indirectly to transmit, publish, link to otherwise make available any confidential information or trade secrets of any person or empathy. You shall not post, publish, transmit, link to, otherwise make available re-transmit or store material on our through any UPC systems, services or products and/or undertake any activity, which infringes or breaches any third party intellectual property rights (which shall include but not be limited to copyrights, trademarks, design rights, trade secret patents, rights of privacy and publicity, moral rights and performance rights). For the avoidance of doubt, the installation or distribution of "pirated software" or other software products that are not appropriately licensed to the customer will constitute a violation of intellectual property rights. In the event of any disagreement as to whether materials posted, transmitted, re-transmitted or stored by a customer or in contravention of this section, the decision of UPC shall be final."

53. The Court finds as a matter of fact that UPC has no interest in doing anything other than making deceptive noises by reference to its acceptable usage policy. Unlike in the case of a non-payment of a bill, UPC intends to do nothing about copyright piracy. In an email of 3rd February 2009 the following appears as the attitude of UPC:-

> "To come back to you all on this and provide feedback from today's SMT: Firstly, we have no comment to make on the Eircom/IRMA agreement – this is a confidential agreement between those two parties and is only of relevance to them. AMB has an old (Corp agreed) holding statement that will continue to be used for any immediate query on p2p generally (ie not this case). Secondly, to confirm we make no reference to this case, nor should speculate as to why we think users might be exceeding their bandwidth capacity in the context of moving customers up to new products tiers. Finally, Regulatory determine if any further action can be gleaned from Eircom's legal strategy on the case above. SMT indicated no other action required for the time being."

54. In a further dishonest reference at high level within UPC to confuse the newspapers and radio and television media, UPC decided to effectively hide its own policy so that no responsible journalist would have the material to ask difficult questions. This email, dated 5th March 2009, states:-

> "Sorry, one last small change to the 4th bullet: I deleted reference to a probably ""policy"", to avoid anyone asking for a copy."

55. This is a requirement from the very top of UPC, as an international company, to require no reference to its own anti-copyright theft customer policy. I emphasise that neither Conor Harrison nor Anna Coyle were the author of any of these distasteful communications. Instead, it is apparent that they are working for an organisation which has possibly not thought through how unfair this approach is. The actions of UPC must be now analysed as to whether their conduct of their business is lawful.

56. The Court is not to be involved in the grant of injunctive relief in the on-going role of supervision. Instead, were UPC, or any other company, to be willing to pursue internet theft by discouraging it through detection and the interruption of transmission, that would clearly be possible. The evidence establishes this with abundant clarity. UPC have presented evidence that their cooperation with a three strikes and then cut off solution, or a diversion solution, or an interruption solution, would be costly and disproportionately difficult. I can accept none of that evidence. It suffices to say that were these solutions to present as economically attractive, UPC would pursue them. In the dispute between EMI and Eircom, which was settled as previously indicated, a pilot project is underway over three months, with a view to determining the final modalities of the solution. This, the evidence establishes, will not cause excessive expense and will, I am convinced by the evidence put before the Court by Mr. Michael Walsh, be possible and practicable.

57. Further, none of the other solutions would be disproportionately expensive in time or expense. None of the contradicting evidence from UPC establishes in any way that I can accept that any such solution would be disproportionately expensive or burdensome. On the contrary, the basic systems of customer interaction are already in place. The excuses given are empty. In order, however, to grant an injunction, the court must be satisfied that it is just and convenient to impose a particular and specific solution on parties to litigation. An analysis should therefore be conducted as to whether other steps are open to the recording companies. The legal basis of injunctive relief, should no other remedy be legally available, then requires analysis.

Alternatives to an Injunction

58. It is definitively established by the evidence that, without the assistance of UPC, the recording companies cannot discover the identity of those who are infringing their copyright. Once that IP address is communicated to UPC as infringing copyright, by the recording companies which find an infringement, they can readily search in respect of the time and date, thereby finding the

subscriber over whose line the infringement took place. Whereas this process does not now appear to be automated, there is nothing in the evidence to suggest that the ordinary application of ingenuity to save time and money, the very essence of computer technology, cannot readily be applied to make this search a simple and inexpensive process. Any suggestion to the contrary in the evidence, I reject.

59. In *Norwich Pharmacal v. Custom and Excise* [1974] A.C. 133, the House of Lords in a different context, established the right of a person who claimed that a civil wrong had been perpetrated to obtain a court order against a party holding information that would enable the identification of the wrongdoer. Thus, for instance, where a car accident takes place, and a proposed plaintiff knows no more than a registration number, were this number not publicly available, or subject somehow to confidentiality, that proposed plaintiff could bring an action against the licensing authority to uncover the name and address of the party alleged to be responsible for the accident, so that an action might be brought.

60. It is established beyond doubt in this jurisdiction that *Norwich Pharmacal* orders are available in the appropriate circumstances. In *EMI v. Eircom Limited* [2005] 4 I.R. 148, Kelly J. made a number of orders whereby the plaintiff in that action, who are also the recording company plaintiffs here, compelled Eircom, as an internet service provider to disclose the names of its infringing customers. The plaintiffs made the case successfully that their copyright had been infringed and demonstrated a series of IP addresses of the responsible subscriber. The judgment of Kelly J. declares that where a wrongful activity has been committee by unknown persons, an order may be made requiring a defendant to identify such persons for the purposes of legal action.

61. In the Federal Court of Appeal in Canada case of *B.M.G. Canada Inc v. Doe* [2005] FCA 193 Sexton J. speaking for the Court, said at paras. 40 to 42:-

> "Intellectual Property laws originated in order to protect the promulgation of ideas. Copyright law provides incentives for innovators - artists, musicians, inventors, writers, performers and marketers - to create. It is designed to ensure that ideas are expressed and developed instead of remaining dormant. Individuals need to be encouraged to develop their own talents and personal expression of artistic ideas, including music. If they are robbed of the fruits of their efforts, their incentive to express their ideas in tangible form is diminished.
>
> Modern technology such as the Internet, has provided extraordinary benefits for society, which include faster and more efficient means of communication to wider audiences. This technology must not be allowed to obliterate those personal property rights which society has deemed important. Although privacy concerns must also be considered, it seems to me that they must yield to public concerns for the protection of intellectual property rights in situations where infringement threatens to erode those rights.
>
> Thus, in my view in cases where plaintiffs show that they have a bona fide claim that unknown persons are infringing their copyright, they have a right to have the identity revealed for the purpose of bringing action. However, caution must be exercised by the courts in ordering such disclosure to make sure that privacy rights are invaded in the most minimal way."

62. The judgment of Kelly J. and the judgment of Sexton J. uphold the basic principle established in the *Norwich Pharmacal* case that where a person, perhaps without fault, get entangled in the tortious acts of others in a way that facilitates their wrong-doing, while no personal liability may be incurred, a duty is establish to assist the person wronged by disclosure of relevant information and of the identity of the wrong-doer. *Norwich Pharmacal* orders are therefore clearly established as an alternative to this injunctive relief. The evidence establishes, however that this process is burdensome and, ultimately, futile as a potential solution to the problem of internet piracy. Helen Sheedy has given evidence of the time, trouble and expense involved in the pursuit of this remedy. That remedy would become simple and inexpensive if appropriate legislative intervention occurred, placing such an obligation by law on the internet service providers by inexpensive application to the District Court. This obligation, for instance, has been imposed in other European countries as a preferred solution to internet theft. After obtaining orders in the High Court, each of the prospective defendants were written to and the evidence against them was put to them. Proceedings were issued in only three cases. In one case the recording companies were satisfied the person was not liable at all. In the two other cases the proceedings were settled, one of which related to a son who had left his father's home. To identify 17, 49 and 23 names, through the three cases seeking *Norwich Pharmacal* orders, cost €680,000 to pay solicitors and barristers on all sides. Some settlements were effected, returning €80,000. The other alternative open is that of information campaigners to educate the public. This did not work. There were international and local press releases at the time of these cases. For a month or two an impact was observed on the incidences of infringements. They quickly returned to their previous level as if nothing had happened.

63. The response of the persons contacted by the recording companies' solicitor in consequence of their names being discovered was described thus by Mr. Sheedy:-

> "The largest single category were the children of the individuals we communicated with. I was surprised, there were a number of professional firms and the horror when they found out what was going on in their premises, I completely believed that they didn't realize that it was going on. In one case this company [Boss] had an internet line which was shared with his own and his son at home was doing it but it looked like his firm was doing it. In another case an employee, a secretary of the firm, was doing the uploading on her company's time… in the great majority [it was young people downloading music]. There were some older people who felt they had the right to do it and a lot of older people told me they had the right to do it."

64. It thus emerges from Ms. Sheedy's evidence that in the vast majority of cases, in this random sample of 17, 49 and 23 illegal downloaders, between the years 2005 and 2007, that there was a willingness to desist on being faced with the threat of court proceedings. I take this evidence into account when considering the graduated response solution to the problem posed by internet piracy.

65. This evidence convinces me that there is no just or convenient solution open to the record companies other than seeking injunctive relief against the internet service provider, in this case UPC. It is argued by UPC, that were injunctions to be granted rights of privacy would be infringed and that an injunction would be disproportionate to the menace that internet piracy represents.

Privacy

66. The existence of a right to privacy is not in doubt; as Hamilton P. in *Kennedy v. Ireland* [1987] I.R. 587 put it, '[t]he right to privacy is not an issue, the issue is the extent of that right or the extent of that right "to be left alone". It has been consistently invoked in the courts over the years; see, for example, *X v. Flynn* (Unreported, High Court, Costello J., 19th May, 1994) and *Re Article 26 and the Employment Equality Bill* 1996 [1997] 2 I.R. 321. Despite this, privacy as a right is difficult to define adequately. The Irish courts have grappled with the scope of the right since it was first recognised in *McGee v. Attorney Genera*l [1974] I.R. 284

as an unenumerated right, flowing from the State's undertaking to defend and vindicate the personal rights of every citizen under Article 40.3.1 of the Constitution. Privacy in the modern panoptic society must be flexible enough to address new technologies and developments and their privacy implications while at the same time certain enough as to offer guidance and clarity as a matter of law. Keeping this tension in mind, it is extremely difficult to arrive at an appropriate definition. Description is therefore preferable.

67. The right to privacy has been said to encapsulate the 'right to be left alone' (per Walsh J. in his dissenting judgment as a judge of the European Court of Human Rights in *Dudgeon v. United Kingdom* (1981) 4 E.H.R.R. 149) or as "the fundamental value of personal autonomy" (per Sedley L.J. in *Douglas v. Hello!* [2001] 1 Q.B. 967 at para. 126) – the right of the individual to exercise control over information, possessions and conduct of a personal nature and, as an obvious corollary, the right to prevent others from accessing this information. On an international level this State is a signatory to various treaties which clearly enumerate the right to privacy. The most important of these is contained in Article 8 of the European Convention on Human Rights which provides, inter alia, that "[e]veryone has the right to respect for his private and family life, his home and his correspondence". This right to 'be left alone' has spawned a considerable amount of data protection legislation, most noticeably at a European level (See, for example, Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data O.J. L 281 23.11.1995 ["the Data Protection Directive"]) and on a domestic level, principally through the Data Protection Act 1988, as amended.

68. I find it impossible to recognise as a matter of constitutional law, that the protection of the entitlement to be left in the sphere of private communications could ever extend to conversations, emails, letters, phonecalls or any other communication designed to further a criminal enterprise. Criminals leave the private sphere when they infringe the rights of other, or conspire in that respect. Legislative intervention may mean detection involves a statutory infringement: leaving the admission of evidence to be decided on the balance of respect for the law and the seriousness of what is involved. In the case of internet file sharing to infringe copyright, I am of the view that there are no privacy or data protection implications to detecting unauthorised downloads of copyright material using peer-to-peer technology; (see, *EMI Records (Ireland) Limited v. Eircom Limited* [2010] IEHC 108, (Unreported, High Court, Charleton J., 16th April, 2010). In this regard, I am taking into account the fact that the process of detection through DtecNet is essentially anonymous. As previously emphasised, a communication between the recording companies and an internet service provider, having used the facilities offered by the DtecNet, that in a particular month a certain one hundred subscribers downloaded an average of twenty copyright protected tracks each, illegally, giving a date and time and the IP address, discloses no information publicly. The recording companies do not thereby harvest the names and addresses of infringers of copyright for data purposes, or for future communication or for evidence in a potential criminal case. They get nothing apart from a set of numbers. As between UPC and their customers, any solution to this illegal activity is conducted privately as between them. They already know each other, as they are joined by a contract. That communication is within the range of matters over which an internet service provider is entitled to deal with its customer. The abuse of an internet service for copyright theft is a serious matter from the point of view of the general enforcement of copyright protection. An internet service provider is entitled to have a policy against it. In this instance, it is apparent that UPC pretends to have such a policy. The existence of a genuine anti-piracy policy would enhance the public standing of any corporation and is a matter in respect of which they have an interest. Enforcing a private contract, in this context, does not have privacy implications. Any form of blocking on that customer and internet service provider basis does not carry a privacy implication. If the response is a graduated one, as opposed to a blocking of communications merely on a basis of identifying its nature and the relevant IP number, no privacy implication arises. As Professor Nixon put it:-

> "If to achieve the goal of identifying that you have to do other things, like store the IP addresses of where it came from and where it went to, and various other things, and you are spotting those for infringing and non infringing uses, then I would start to worry about that information being stored, and how it is being used, for what purposes… In a graduated response, they are not, the DtecNet guys are looking at every communication that goes through the UPC network. What they are doing they are joining a particular stream of communications that is in this peer-to-peer network, which has by default at this moment in time, lets say 60%, 70%, 90% of the people who are on it are sharing infringing material, and you pick those people and you store the information. Now I don't think so - I think that is reasonable… nobody is exposing anything in these networks, apart from the fact that they have an IP address, some made up user name, and the files that they are infringing, or the files they are not infringing. So, that information is made publicly available [over the network anyway] so, that is fine."

69. Mr. Sehested had a similar view. He said:-

> "I mean all of the information that we capture is publicly transmitted information that anyone with an internet communication and a peer-to-peer programme, that is freely downloadable, would be able to capture. Again all the files that we capture here are files that are actively made available by the users… [i]n this case specifically we are solely looking for sound recording. So we only look for content that is part of that file that we have been given to monitor for."

70. That evidence is the basis of my conclusion that the right of privacy is not engaged by the scrutiny of files publicly made available for copyright theft on the internet and nor is it engaged by deep packet inspection for the purpose of detecting and diverting or disenabling such transmissions.

Response to Warning

71. The evidence establishes that detection, Solution I, followed by warning over three occasions and eventual discontinuance of internet access will succeed in strongly alleviating the problem of internet piracy. There is a strong probability that a graduated response would yield a majority level of desistance from the practice of illegal downloading on a first warning. In that regard, I take into account the evidence of Charles Benjamin, of Anna Coyle, of Professor Nixon and Helen Sheehy. Within an Irish context, the most convincing evidence I heard was that of Helen Sheehy. In response to the *Norwich Pharmacal* orders, the majority of people were described as being embarrassed that they or their family had stolen copyright material when first communicated with. Those who were responsible tended to admit the fact; and some were being made aware that a practice in which they disapproved has been carried out through family members. A survey was put to Professor Nixon whereby it was indicated that seven out of ten people would cease internet piracy if warned. His response, in that regard, was appropriately cautious. He noted that there was hope that most people would alter their behaviour. Within the realm of a university, from which perspective Mr. Benjamin spoke, the situation is persuasive, though not precisely comparable. The result of the University of Florida policy not to tolerate internet piracy over their network has been an extremely high level of response on the first warning of those warned; only 1% went to the final level whereby they were required to consult with a disciplinary officer within the University. Mr. Benjamin is of the view that even if the system which he employed was not achieving 100% detection, that it was certainly achieving detection of repeat offenders. Bringing this process partly out into the open, where by internet thieves are privately communicated with, can be predicted in most instances to shame them out of their behaviour. They then become as the seller of pirated DVDs outside the cinema. I reject all UPC evidence to the contrary. In the situation of general internet service provision in Ireland, those who are determined may tend to ride out the warnings, to offer excuses in relation to violations, to seek a ruling against their provider and, if unsuccessful, to move to one of

another dozen or so internet service providers. I am satisfied that these persons will be in the small minority. Further, I am satisfied that the current age profile for internet piracy indicates a use of home computers at a residence where at least some of those involved are subject to family admonition. Others will be embarrassed at being detected. The evidence establishes that this will make up a substantial majority.

General Record

72. The recording companies are, as a matter of preference, seeking an injunction from the Court whereby, on a third detection of infringement, on a month-by-month basis for each infringement, the person involved will be barred from any internet access. There is no general register for those who are cut off from internet service for not paying their bills. I am satisfied from the evidence of Anna Coyle, that there is some degree of informal communication, but that if it happens, it is rare. There is no plea in this case that a general register should be created of those who have been cut-off from internet access due to failure to pay a bill or due to repeated violations of a prohibition against internet piracy. To set up such a register may well have data protection implications. I do not need to comment on any issues that might so arise. As the solution is now proposed, there is no disproportionality.

Warning

73. A warning can be important in the adjudication of whether an injunction is to be justly granted. Much correspondence has been exchanged between the parties. This, on the one hand, makes the case that the network of UPC is being used by its customers to infringe the copyright held by the recording companies. UPC, on the other hand, demonstrates in its written replies, a careful series of arguments to the affect that they are merely a conduit between its customers and others. Furthermore, they argue that the Copyright and Related Rights Act 2000 does not allow for the making of an injunction against them or require them to take action, in respect of copyright piracy since s. 40 of the Act declares in subs. (3) that the provision of facilities for enabling the making available to the public of copies of a work does not of itself constitute that action. It is where a person who provides facilities is notified by the owner of the copyright in the work concerned, that such facilities are being used to infringe copyright in that work, then unless the person so notified, removes the infringing material as soon as practicable, then liability for copyright infringement is established under subs (4). Solely at issue is whether the recording companies have notified the UPC that its facilities are being used to infringe copyright. As to whether this constitutes the making available to the public of copies of a work and as to whether any of the solutions deposited by the recording companies to peer-to-peer internet piracy of their work constitutes a step "to remove that infringing material" is a separate matter, dealt with later in this judgment.

74. By letter dated 13th February 2009, Helen Sheehy, on behalf of the recording companies, made the case that the law obliged UPC to act in the manner similar to the agreement reached with Eircom in January 2009. The parties there contracted for a three stage response to internet piracy. The recording companies were to alert them to infringements through the use of DtecNet on a month-by-month basis. If, in the first month, an infringement was notified in the appropriate format, Eircom were to write to its customers by way of an education policy; as to the possibility of the misuse of a network by an employee, family member or, possibly, someone within the range of their wireless router. On a second infringement, a sterner letter was to be written. On a third infringement, the customer was to be disconnected as to broadband internet access, but not as to telephone and television services received over the internet and not in the case of business customers or those dependent upon the internet for serious medical reasons.

75. By letter dated 27th February 2009 UPC declared:-

> "For the avoidance of doubt UPC Ireland does not condone illegal file sharing and our policies, procedures and terms and conditions of service ensure that the company complies with all prevailing laws in Ireland. UPC has recently taken legal steps to prevent various forms of copyright infringement of content on our cable and MMDS network, therefore, be assured we are motivated to address illegal activity on our networks in general, including piracy and copyright infringement. On that basis we are happy to discuss with your clients and all other stake holders on a multilateral basis (to include other rightholders, fellow ISPs the Data Protection Commission, Consumer and Piracy Groups etc). Any practical initiatives that can be taken to address the concern of the illegal file sharing within the confines of the law. The measures proposed in your letter are, however unacceptable and do not take account of the rights and interests of subscribers and ISPs and we cannot agree these as a basis for discussion. Moreover, it appears your request is that we should simply agree to sign up to a similar private arrangement that you have with another party…"

76. As has emerged, I am not at all satisfied that the response by UPC was genuine. It is apparent that UPC vigorously pursue customers who exceed the limit on their broadband package, and charge them more on a unilateral basis in appropriate cases. This provision of their acceptable usage policy is pursued entirely on a profit motive basis.

77. By letter dated 14th May 2009, Helen Sheehy, on behalf of the recording companies, formally put UPC on notice, that their facilities were being used to infringe copyright in sound recordings owned by the recording companies. In part, the letter reads:-

> "We are of the view that UPC is on notice of illegal file sharing on its network, following upon the High Court disclosure action reference number 4368P/2005. Since our letter to you dated the 13th February 2009 random scans of the peer-to-peer to activity on your network show that the activity is continuing. I enclose details of random samples of illegal peer-to-peer activity on Direct Connect, Gnutella and Ares protocols on the UPC network for March and April of 2009. Our clients are of the view that your failure to remove illegal material, when you are aware that it is on your network, and constantly travelling through your network has the effect of making you also liable for copyright infringement pursuant to s. 40(4) of the Copyright and Related Rights Act 2000. We are calling on you now to remove infringing material from your network and whilst the manner in which you do this is matter for you. We… are suggesting that this may be done as was done by Eircom by agreement with copyright holders who are prepared to work with you to stop the massive breaches of copyright taking place on your network. If you are not prepared to remove illegal material from your network then we have no option but to take legal action to protect our client's rights."

78. I am satisfied on the evidence that a number of scans were conducted on some 350 popular tracks over a few days in March and April of 2009. I am also satisfied that the evidence establishes definitively that the UPC internet network was then being used, and is now being used, for the illegal copying of valuable copyright material owned by the recording companies. I am satisfied that this abuse is widespread and, as analysed elsewhere in this judgment, constitutes the majority use, if not the great majority use, of peer-to-peer traffic.

79. The material enclosed showed first of all a case summary indicating user name, IP address, date of when the user was last online, downloaded files and the internet service provider to whom the relevant IP address was assigned. On the 18th May 2009, UPC replied that the individuals "may or may not be our customers". That is not an honest answer. It was denied that there was any infringing material on the network and, instead, it was stated that what was involved was merely the provision of "information that our customers may be using our network to access certain allegedly infringing material". The letter goes on to state that UPC "has no

liability for the actions of our customers in this regard as we are a mere conduit." Section 40(4) of the Act is referred to as "a take down provision designed to address infringing material hosted by facilities providers".

80. Further information was provided from the UPC solicitor by letter dated 26th May 2009. This time, a file of information as to the use of the UPC network for infringing copyright material was added to the letters.

81. By letter dated 2nd June 2009, the solicitors on behalf of UPC reiterated that their client was a mere conduit and, therefore, not liable to injunctive relief. The letter indicated that there was a right of communication to the public and that injunctive relief was not available under Irish law. In particular they stated that an injunction could not be granted on a non-individualised basis "through an unverified, automated process". In that regard, the Court would comment that the DtecNet system of infringement has, as is stated elsewhere in this judgment, being demonstrated to be accurate. Further, there was no question put which undermined the reliable nature of that system.

82. On any graduated response to infringement, the letter continued:-

> "We consider that such an approach would be inconsistent with the recent re-introduction by the European Parliament of Amendment 138/46 to the current proposals to revise the European Telecoms Regulations (which we understand are in principle supported by the Irish Government), which will make it illegal for any EU member state to introduce legislation that would allow a citizen's internet connection to be disconnected without first being found guilty in court. This principal would also prevent any inter-industry agreement that facilitated the disconnection of a citizen's internet access without a court order. As a result, there is no basis for your client to pursue with other ISPs a graduated response system in similar terms to that agreed with Eircom.
>
> Our client takes the rights of its customers very seriously, including in the areas of data protection and privacy. Our client will of course comply with any court order your client's may obtain in respect of a particular customer of our client that is held to be infringing our client's copyright. In addition, in incidents where our client may provide hosting facilities, our client will continue to comply and enforce the applicable notify and take down policy in appropriate circumstances.
>
> Finally, for the avoidance of doubt, our client's reference to "key stake holders" has been consistent throughout our client's correspondence and such stake holders were enumerated in particular in our client's letter to you of 27th February 2009. In spite of our client's view that it has no liability for the copyright infringement of its customers, if any, for the reasons set out above, our client confirms that it would be prepared to participate in a discussion process with all stake holders on the issue of illegal file sharing which is convened by your clients. We note however, that our client will only participate on the basis that any proposals are consistent with the European Parliament's proposals set out above and with the general principles that network access should only be disabled in accordance with an order of the Court."

83. Having regard to the entirety of this correspondence the Court is satisfied as to two matters. Firstly, there has been notification to UPC within the meaning of s. 40 of the Act. Secondly, there has been no reasonable offer of engagement by UPC with a view to eradicating or substantially diminishing copyright piracy. In this regard, the Court fully accepts the evidence of Dick Doyle. The evidence analysed in the course of this judgment also establishes that detection, warning and discontinuance are, each of them, proportionate to the vast scale of the problem established in evidence.

84. I now turn to the relevant principles for the grant of an injunction and proceed to analyse national law, in the context of our European legal obligations, and contrast the measures in place in Ireland with the legislation in Europe and the United States of America.

Authority of the Court

85. An injunction is never available simply because the Court deprecates a situation or has no respect for the defence offered to participation in a grave economic wrong against copyright holders. In the course of argument, mention was made of the constitutional protection afforded to copyright: in particular, in Phonographic Performance Ireland Limited v. Cody [1998] 4 I.R. 504, Keane J. at p.511 stated that the right to be identified with a creative work, and to enjoy protection whereby others are not allowed to copy it without permission was protected by the Constitution:-

> "The right of the creator of a literary, dramatic, musical or artistic work not to have his or her creation stolen or plagiarised is a right of private property within the meaning of article 40.3.2° and Article 43.1 of the Constitution of Ireland, 1937, as is the similar right of a person who has employed his or her technical skills and/or capital in the sound recording of a musical work. As such, they can hardly be abolished in their entirety, although it was doubtless within the competence of the Oireachtas to regulate their exercise in the interests of the common good. In addition and even in the absence of any statutory machinery, it is the duty of the organs of the State, including the courts, to ensure, as best they may, that these rights are protected from unjust attack and, in the case of injustice done, vindicated."

86. The courts must defer, however, to the manner in which the Oireachtas circumscribes and regulates the enforcement of those rights. The Court is bound, in that regard, the matter having been considered by the Oireachtas, to apply the law within the four corners of the Copyright and Related Rights Act 2000. It might be possible to argue that in the absence of such protection, that the Court was mandated to use the amplitude of its powers in order to vindicate the injustice that is at the heart of this case. Further, it might be possible to argue that even in the absence of a primary actionable wrong that an injunction might be granted in relation to a morally indefensible action; see *Prince Albert v Strange* (1849) 2 De & Sm 293 where an injunction was granted for breach of confidence, not then a defined tort, and, more recently, *Douglas v Hello!* [2002] 2 A.C. 457. To act in this way, however, would be to ignore the power of the Oireachtas to regulate rights in accordance with a just scheme of legislation that balances the exercise of those rights with the responsibility of living within an ordered society. In some rare instances, the courts may also directly enforce Bunreacht na hÉireann through injunctive relief where no remedy is already set out in law. The courts are not entitled, on the other hand, to take an area which has been properly legislated for as to the extent and balance of rights by the Oireachtas and to take a different view. For the Court to pursue the course of granting an injunction on the basis not of law but of economic abuse or moral turpitude would lead the Court beyond the threshold of the judicial arm of government and into legislation. It would undermine respect for the rule of law: for no one would know quite what the rule of law might be if it depended on attitudes forged through legal argument in individual cases as to what was acceptable conduct. The danger that would arise would be that the Court could then be described by reasonable people as acting on the basis of preference, were the Court to use any wider and wrongly assumed right to injunct behaviour in the same way that the tort of conspiracy was historically used against trade union action by judges in England in the late 19th and early 20th centuries, up to the passing of the Trade Disputes Act 1906, and some would argue, beyond.

87. Therefore, the only proper response to this problem is to consider the precise scope of the legislative framework as set out in the

Act and whatever aspect of European legislation might legitimately be used as an aid in interpreting national law.

88. I therefore turn to the legislation.

The Right to Copy
89. Section 17 of the Copyright and Related Rights Act 2000 definitively indicates the extent of the constitutional right to own creative work:-

> "17(1) Copyright is a property right whereby, subject to this Act, the owner of the copyright in any work may undertake or authorise other persons in relation to that work to undertake certain acts in the State, being acts which are designated by this Act as acts restricted by copyright in a work of that description.
>
> (2) Copyright subsists, in accordance with this Act, in
>
> (a) original literary, dramatic, musical or artistic works,
>
> (b) sound recordings, films, broadcasts or cable programmes,
>
> (c) the typographical arrangement of published editions, and
>
> (d) original databases.
>
> (3) Copyright protection shall not extend to the ideas and principles which underlie any element of a work, procedures, methods of operation or mathematical concepts and, in respect of original databases, shall not extend to their contents and is without prejudice to any rights subsisting in those contents.
>
> (4) Copyright shall not subsist in a work unless the requirements for copyright protection specified in this Part with respect to qualification are complied with.
>
> (5) Copyright shall not subsist in a work which infringes, or to the extent that it infringes, the copyright in another work.
>
> (6) Copyright shall not subsist in a work which is, or to the extent that it is, a copy taken from a work which has been previously made available to the public."

90. Chapter 4 of the Act defines the rights of the copyright owner, the most profound of these is to be identified with the work. From the point of view of legitimate reward for creative effort, the right to make copies of a work available to the public is vested in the maker of the work by the following section of the Act:-

> "37(1) Subject to the exceptions specified in Chapter 6 and to any provisions relating to licensing in this Part, the owner of the copyright in a work has the exclusive right to undertake or authorise others to undertake all or any of the following acts, namely:
>
> (a) to copy the work;
>
> (b) to make available to the public the work;
>
> (c) to make an adaptation of the work or to undertake either of the acts referred to in paragraph (a) or (b) in relation to an adaptation,
>
> and those acts shall be known and in this Act referred to as "acts restricted by copyright".
>
> (2) The copyright in a work is infringed by a person who without the licence of the copyright owner undertakes, or authorises another to undertake, any of the acts restricted by copyright.
>
> (3) References to the undertaking of an act restricted by the copyright in a work shall relate to the work as a whole or to any substantial part of the work and to whether the act is undertaken directly or indirectly."

91. Under s. 43 no one is entitled to infringe copyright by adapting a work. Under s. 42 lending rights are restricted. Under s. 41 the author of the work can restrict circulation, whether by sale, rental or loan, or otherwise of the work. Under s. 39 the right of the owner to control the reproduction of the work is defined. This concept of reproduction includes the storing of the work in any medium, or making copies which are transient. A two dimensional work may not be copied in three dimensional format, and vice versa. Photographing a film or television broadcast is prohibited. Copying a recording or a music score is clearly prohibited. Changing the typeface in a literary work does not escape copyright. Under Chapter 8 of the Act, copyright is assignable from the owner and is transmissible by will. Chapter 9 of the Act deals with the remedies available to copyright owners. These include quite draconian remedies of seizure; of obtaining a declaration from Court that ceased copies of a work are no longer the property of the copyright thief, but of the owner; and include rights to take possession of equipment used to infringe copyright. The described provisions are set at nought by internet theft, unless it can be stopped. Furthermore, the declaration by the European Union of the entitlements that are to be ascribed in copyright to the creative community, and which are partly expressed in Irish legislation, become futile in the absence of remedies that bypass internet abuse or which set up internet access as being a superior right attracting entitlements to which no other area of infringement would adhere. Among the remedies in favour of the author declared in the Act are those to damages, and to an injunction. Section 27 provides that rebroadcasts, except by the programme makers, for instance of live music, are to be prohibited:-

> "27(1) The copyright in a broadcast shall expire 50 years after the broadcast is first lawfully transmitted.
>
> (2) The copyright in a repeat broadcast shall expire at the same time as the copyright in the original broadcast and no copyright shall subsist in a repeat broadcast which is transmitted after the expiration of the copyright in the original broadcast."

92. Briefly, as has been described in detail in this judgment, the form of copyright theft at issue here is by peer-to-peer sharing. There, the copies of the work sit in the home computers, in some instances the work computers, of many millions of individuals. By joining a swarm, in the manner described by Mr. Kavanagh in evidence, the material available on those computers is taken through

various networks, and ultimately in respect of UPC customers, through the UPC network into the computers of the persons seeking the download. The parties making available copies of their work, because the system is two-way, include the downloader and those from whom he or she uploads. I have no doubt, therefore, that it is not UPC that is making available copies of the work. The work does not reside on their network, since they do not store it, host it or cache it, terms explained later in this judgment, but are merely a conduit for it. This, nonetheless, profoundly affects the right of the copyright owner to make available copies of the work to the public. The crucial issue is whether the Act allows the Court to interfere with the transit through the UPC network of copyright music to those intent on stealing it and offering it for theft on their home computers. Section 40(1) of the Act declares:-

> 40(1) Reference in this Part to the making available to the public of a work shall be construed as including all or any of the following, namely:
>
> (a) making available to the public of copies of the work, by wire or wireless means, in such a way that members of the public may access the work from a place and at a time chosen by them (including the making available of copies of works through the Internet);
>
> (b) performing, showing or playing a copy of the work in public;
>
> (c) broadcasting a copy of the work;
>
> (d) including a copy of the work in a cable programme service;
>
> (e) issuing copies of the work to the public;
>
> (f) renting copies of the work;
>
> (g) lending copies of the work without the payment of remuneration to the owner of the copyright in the work,
>
> and references to "lawfully making available to the public" shall mean the undertaking of any of the acts referred to in paragraphs (a) to (g) by or with the licence of the copyright owner."

93. To crystallise these rights for the purpose of analysis, I take an example. A very entertaining crime novel called "Degrees of Guilt" was published last June in London, and the author is Patrick Marrinan. His copyright in that work lasts for his lifetime and seventy years. It is the kind of thriller that may be attractive to film companies, and could easily be adapted into a play. The author's right to make copies available would be infringed were a copy of the book to be hosted on the internet; were the book to be read in public; were the book to be broadcast on television or radio as a reading; were that to be included in a cable, television or radio service; were the book to be photocopied as to any substantial part or, more obviously, reprinted and sold; were the book to be rented out; or copies of the work lent without any remuneration to the author. The author's rights would also be infringed by an adaptation into a film or a play or a musical or a computer game; see s. 43 of the Act.

94. All of these activities require to be facilitated by people other than those who are directly intent on breaching copyright. Equipment is needed for the purpose. The film would require actors and cinematographers before being shown in a cinema; the play would be shown in a theatre; the book would be photocopied on a machine; or printed by a printer; the broadcast would take place through a network; and the pirated copies would be made available through the internet, either from a hosting site, or in the case of peer-to-peer transmissions, from the home computers of many individuals. Providing facilities for this activity is not, of itself, a breach of copyright. Section 40(3) of the Act provides:-

> "40(3) Subject to subsection (4), the provision of facilities for enabling the making available to the public of copies of a work shall not of itself constitute an act of making available to the public of copies of the work."

95. This section, in its ordinary construction, applies to any of the activities described in s. 40(1). Facilities are needed, including an internet service provider, to access a host site containing the work, or to access peer-to-peer copies of the work residing illegally on home computers. Facilities are also needed to perform a work in public or to broadcast it, put it on a cable programme service, print it without permission, rent it out, or lend copies. The facilities needed will, in each case, differ. In the case of a library, the situation is simple. The library is a facility whereby copies of "Degrees of Guilt" are made available. That is a present and a continuing threat to the rights of the author where he has not so given permission. In the case of the hosting site on the internet, or a pay for access cable radio or television service, the work is on the internet site or in the computer storage facilities of the media company. What can be done about any of the situations is specified in the legislation. Liability is not established, unless there is a warning to the individual or company providing facilities that enable copyright infringement. Even then, the right of the Court to take action, is severely circumscribed by the wording itself. The exception from liability for copyright infringement provided in subs. (3) is qualified in subs (4), so that action can only be taken as follows:-

> "(4) Without prejudice to subsection (3), where a person who provides facilities referred to in that subsection is notified by the owner of the copyright in the work concerned that those facilities are being used to infringe the copyright in that work and that person fails to remove that infringing material as soon as practicable thereafter that person shall also be liable for the infringement."

96. This subsection is to be construed within its context. Its meaning is to be primarily ascertained from the language chosen by the Oireachtas whereby its intention is conveyed. Where a provision is obscure, ambiguous, or a literal interpretation would be absurd, or would fail to reflect the plain intention of the Oireachtas, that intention should be ascertained from the Act itself, in order to give effect to the purpose of the legislature; s. 5 of the Interpretation Act 2005. If the meaning of the text is, however, unambiguous, the task of the court is to give effect to that literal meaning. The court is not entitled to give an opinion as to sound policy by way of a judgment, much less give effect to it, but, rather, to implement the intention of the Oireachtas. Even though a deviation from the plain meaning expressed may be desirable, the court has no authority to pursue any course which would involve rewriting the text. That approach undermines the rule of law, which is based on predictability and on the separation of powers.

97. Words are not to be presumed superfluous. Rather, I start from the position that effect should be given to all of the words within a section, or subsection, where that is possible. While sometimes, in the way that lawyers offer pleadings in the alternative, such as a claim for breach of duty and a claim for negligence, the Oireachtas might well be drawn into the use of words with a view to emphasising certainty, the ordinary rule as to economy in the use of language should be applied. An ordinary word should be given an ordinary meaning but, at times, I find the use of a dictionary helpful in clarifying an interpretation. The Act contains a number of specialist terms. These are to be given a technical meaning, but are not, beyond the use of the word internet, germane to this

decision. I have been assisted in this analysis by the expert re-statement of the relevant rules in David Dodd '*Statutory Interpretation in Ireland*' (Tottel, Dublin, 2008).

98. Under s. 40(5), the Minister is entitled to prescribe the form of a notice to be given whereby the person who provides facilities to infringe copyright, and fails to remove the infringing material, becomes liable. The draft regulation made by officials of the Minister has been referred to in evidence. I have no regard to it for two reasons. Firstly, it was never brought into law. Secondly, it constitutes only, at most, a guide to the opinion of one individual on the interpretation of the interrelatedness of subs. (1), (3) and (4) of s.40.

99. In the context of the detailed description of peer-to-peer copyright piracy in this judgment, I ask myself the question, whether internet facilities such as those sold by UPC are being used to infringe the copyright in works owned by the recording company. In the present, though intermittent, sense they are. Each time someone downloads a work from other peer-to-peer users, the facilities of UPC are then being used to infringe the copyright owned by the recording company. This is a process that, for the theft of music takes only seconds, or in the case of a film, some minutes. In a digital sense, that material can then be argued to be on the network of UPC. Blocking a customer by removing his internet access ensures that this process does not take place. That would then ensure that the facilities cannot be used for internet piracy. That is not, however, what the subsection says. When, at night, UPC throttle peer-to-peer communications some packets of information as the start of the process are discarded. I am satisfied, on the evidence, that they are later resent. This is relevant, in the context of the interpretation of how the person or company, whose facilities are being used to enable the making available to the public of copies of a work, is required to remove that infringing material. This is made clear in a passage of cross-examination of Professor Nixon, an expert in computer technology who was called on behalf of UPC but who demonstrated independence of mind, and therefore reliability. Notwithstanding the expertise displayed by Mr. Newman for the recording companies in cross-examination, and the advocacy involved in leading the professor towards a particular point of view, the Court is obliged to construe its overall effect fairly. The passage is as follows:-

> "Q. Well, the level of the individual data packet… is removed from the network. Now the data packet may be resent by the end of the network, but the individual data package is removed by the network?
>
> A. Discarded, removed.
>
> Q. Yes. So does that not suggest then the idea of removal means a little bit of more than the removal from that server?
>
> A. No, you see I don't think it does because the purpose of the discarding of the packets is to change the behaviour of the communication in the case of [deep packet inspection] and throttling and such like. So it is not removing the communication, it is not removing the information that leaves one end and arrives at the other end, it is affecting the overall performance of the communication. If you want to remove the file, you have to remove it at source.
>
> Q. Well when, for instance, the [deep packet inspection appliance] removes an individual packet, it is not removing it from a server, is it?
>
> A. No, it is stopping that piece of data transiting the network. That small component part of it.
>
> Q. So your understanding of removal seems to be very much shaped around the idea of whether it is managing to remove the entire communication or not?
>
> A. The question that was posed is; can you remove a file?
>
> Q. Yes.
>
> A. Can you remove a piece of work? Can you remove an artefact? To do that you need to remove it from the machines that it exists on. We have already established that certainly you stop a communication, but the files still exist on the machines that it existed on before the communication.
>
> Q. For instance, if a file is being transmitted through a network, I suppose perhaps put it this way, if a subscriber's computer is being regularly used, or perhaps continually used for resending infringing material over the UPC network, and then the subscriber stops sending that material over the network, perhaps because they have received a warning or otherwise, then is it not correct that that infringing material, it is removed from the network?
>
> A. Yeah, I mean if it is removed by someone going there or by the individual stopping, it is still removed."

100. The procedure described in detail in this judgment for effecting internet piracy, which involves using UPC as a transit, supports this expert view as correct. Cutting off access to the computers holding pirated copyright songs is not to remove infringing material; it is to stop the transit of that material. Further, as has been analysed in relation to the possible responses to internet piracy, two of the programmes, namely CopySense and Global File Registry cannot fairly, on my analysis, be described as removing material from the internet. Instead, on recognising the file hash of a copyright work, at the speed of light, these programmes strike so as to interrupt the transmission and send a warning, in one case, or in the other, interrupt the transmission and divert the subscriber on to a place where the track sought illegally for nothing can be obtained legally for a small fee. This is not, in the ordinary use of language, the removal of infringing material from the network. Further, as will now be clear, UPC has been warned by the recording companies that its network is being used for the infringement of copyright. It has chosen to ignore these warnings and not to act. By the time the warnings are given, however, although the material may as a matter of high probability again be transmitted from time to time through the network, it is not then capable of being removed. While I do not accept the argument for UPC that s.40(4) of the Act refers only to an internet service provider hosting a copyright infringing site on its network, and while I believe that the removal of infringing material could apply, for instance to DVD lending libraries, the plain wording of the section in its use of the present tense and its reference to removing the infringing material, requires that action should be taken in respect of a then existing situation, not by digital blocking or diverting stratagems, but by removal. That is simply not possible in the context of a transient communication. Perhaps, however, the legislation can be looked at differently in the context of the European law which it has been argued to mirror?

European Obligations

101. I turn therefore to the obligations of the State as a member of the European Union. In that regard, where a Directive places a legislative obligation on the State, most especially where national legislation, as is the case in relation to Act of 2000, is concerned to implement its terms through choice of appropriate measures, that national legislation must be construed so as to conform with its legislative purpose. Thus, a national measure must be interpreted in accordance with the obligation of the State to abide by European law. That obligation arises whether the legislation was brought into law before or after a directive. This is made clear by the judgment

of the European Court in *Marleasing SA v. La Commercial Internacional de Alimentacion SA* [1990] 4 E.C.R I-4135 (C-106/89), where the European Court of Justice held, at pp. 4158-4159:-

> "6. With regard to the question whether an individual may rely on the directive against a national law, it should be observed that, as the Court has consistently held, a directive may not of itself impose obligations on an individual and, consequently, a provision of a directive may not be relied upon as such against such a person (judgment in Case 152/84 *Marshall v Southampton and South-West Hampshire Area Health Authority* [1986] ECR 723).
>
> 7. However, it is apparent from the documents before the Court that the national court seeks in substance to ascertain whether a national court hearing a case which falls within the scope of Directive 68/151 is required to interpret its national law in the light of the wording and the purpose of that directive in order to preclude a declaration of nullity of a public limited company on a ground other than those listed in Article 11 of the directive.
>
> 8. In order to reply to that question, it should be observed that, as the Court pointed out in its judgment in Case 14/83 *Von Colson and Kamann v. Land Nordrhein-Westfalen* [1984] ECR 1891, paragraph 26, the Member States' obligation arising from a directive to achieve the result envisaged by the directive and their duty under Article 5 of the Treaty to take all appropriate measures, whether general or particular, to ensure the fulfilment of that obligation, is binding on all the authorities of Member States including, for matters within their jurisdiction, the courts. It follows that, in applying national law, whether the provisions in question were adopted before or after the directive, the national court called upon to interpret it is required to do so, as far as possible, in the light of the wording and the purpose of the directive in order to achieve the result pursued by the latter and thereby comply with the third paragraph of Article 189 of the Treaty.
>
> 9. It follows that the requirement that national law must be interpreted in conformity with Article 11 of Directive 68/151 precludes the interpretation of provisions of national law relating to public limited companies in such a manner that the nullity of a public limited company may be ordered on grounds other than those exhaustively listed in Article 11 of the directive in question."

102. This is a domestic dispute between undertakings, namely the recording companies and UPC, as to the correct interpretation of national legislation. The applicability of the principle just stated to this kind of dispute is not in doubt. In any event, it is made clear in *Wilhelm Roith v. Deutsches Rotes Kreuz* [2004] E.C.R. I-8835 (C-397/01), in the course of which the European Court of Justice made the following observations:-

> "111. It is the responsibility of the national courts in particular to provide the legal protection which individuals derive from the rules of Community law and to ensure that those rules are fully effective.
>
> 112. That is a fortiori the case when the national court is seized of a dispute concerning the application of domestic provisions which, as here, have been specifically enacted for the purpose of transposing a directive intended to confer rights on individuals. The national court must, in the light of the third paragraph of Article 249 EC, presume that the Member State, following its exercise of the discretion afforded it under that provision, had the intention of fulfilling entirely the obligations arising from the directive concerned (see Case C 334/92 Wagner Miret [1993] ECR I-6911, paragraph 20).
>
> 113. Thus, when it applies domestic law, and in particular legislative provisions specifically adopted for the purpose of implementing the requirements of a directive, the national court is bound to interpret national law, so far as possible, in the light of the wording and the purpose of the directive concerned in order to achieve the result sought by the directive and consequently comply with the third paragraph of Article 249 EC (see to that effect, inter alia, the judgments cited above in Von Colson and Kamann , paragraph 26; Marleasing , paragraph 8, and Faccini Dori , paragraph 26; see also Case C 63/97 BMW [1999] ECR I 905, paragraph 22; Joined Cases C 240/98 to C 244/98 Océano Grupo Editorial and Salvat Editores [2000] ECR I-4941, paragraph 30; and Case C 408/01 Adidas-Salomon and Adidas Benelux [2003] ECR I-0000, paragraph 21)."

103. This principle, it is important to recall, cannot be used beyond the scope of its proper purpose so as impose a solution which, though in conformity with an obligation under a directive, contradicts the plain terms of national law. The obligation of conforming interpretation of national law in the light of any European law obligation must be implemented "as far as possible." This has been explained more fully in the context of the implementation of a Framework Decision in Case C-105/03 *Pupino* [2005] E.C.R. 1-5285 by the European Court:

> "The obligation on the national court to refer to the content of a framework decision when interpreting the relevant rules of its national law ceases when the latter cannot receive an application which would lead to a result compatible with that envisaged by that framework decision. In other words, the principle of conforming interpretation cannot serve as the basis for an interpretation of national law contra legem. That principle does, however, require that, where necessary, the national court consider the whole of national law in order to assess how far it can be applied in such a way as not to produce a result contrary to that envisaged by the framework decision."

104. I must now refer to the complex series of directives concerned with electronic commerce, with copyright, and under the framework within which these rights must be upheld. In doing so I note that in the European Communities (Copyright and Related Rights) Regulations 2004 (S.I. No. 16 of 2004), the explanatory note states that while Ireland was already in substantial compliance with the directives to which I will now refer, that instrument made a number of amendments to ensure full compliance by the State with the relevant European directives. That statement, I regret to say, is in error.

European Directives

105. First of all, insofar as it may be important, a brief chronology. The Copyright and Related Rights Acts 2000, was passed on 10th July and brought into force on 1st June 2001. At that time the E-Commerce Directive, which I will shortly refer to by its full title, had been passed on the 8th June 2000. Article 22 of that directive gave the State up to the 17th January 2002, to implement its terms. European Parliament and Council Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society O.J. L167/10 ("The Copyright Directive") was passed on 22nd May 2001. It was in draft form, and in the contemplation of the legislature, when they passed the Copyright and Related Rights Act 2000. European Parliament and Council Directive 2002/21/EC on a common regulatory framework for electronic communications networks or services O.J. 108/33 ("Framework Directive") was passed on 7th March 2002. The Communications Regulation Act 2002, allowing for regulation of internet service providers by The Commission for Communications Regulation, was passed in the year 2000. This was followed by the European Community (Directive 2000/31 EC) Regulations 2003 (S.I. No. 68 of 2003).

106. European Parliament and Council Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce), O.J. L178/1 17.7.2000 ("the E-Commerce Directive") provides defences to internet service providers who transmit copyright material. These defences arise when an internet service provider establishes that they are a mere conduit, or merely hosting information, as in an internet site, or are caching information, or websites, for instance in order to enable more ready access to popular search targets. The first of these defences is set out in Article 12 of the Directive as to "mere conduit"

> "1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:
>
> (a) does not initiate the transmission;
>
> (b) does not select the receiver of the transmission; and
>
> (c) does not select or modify the information contained in the transmission.
>
> 2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.
>
> 3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

In Article 13 as to "Caching", the following appears as to the scope of the defence:-

> 1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:
>
> (a) the provider does not modify the information;
>
> (b) the provider complies with conditions on access to the information;
>
> (c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;
>
> (d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and
>
> (e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.
>
> 2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement."

And, finally, in Article 14 as to "Hosting", these are the provisions:-

> "1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:
>
> (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
>
> (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.
>
> 2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.
>
> 3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

107. In addition to that, as explained by Recital 47 to the E-Commerce Directive, Article 15 requires that Member States should not impose a general obligation to monitor information. I am satisfied that this is irrelevant to any issue arising in this case. Deep packet inspection, as described in this judgment is not the seeking of information which is in the course of transmission. Instead, it identifies the nature of transmissions, whether encrypted or otherwise, by reference to the ports which they use, and the protocol employed, so as to identify peer-to-peer communication. UPC does this already for legitimate commercial purposes related to the management of transmissions. If it suited, they could also easily identify the file # of copyright works and block them or divert the search in aid of theft to a legal site. This is not a general search for information. It is simple use of deep packet inspection technology in aid of proper transmission.

108. I am satisfied that UPC is a mere conduit. It did not initiate any peer-to-peer transmission, whereby copyright material is stolen; the peer-to-peer swarms select who is to receive the transmission; and, in the course of transmission, the information is not selected or modified. Whereas I respect the opinion offered on this section by Mr. Michael Walsh, on behalf of UPC and regard him as a genuine expert of independent mind, I prefer Professor Nixon's opinion. There is no modification of information in these transmissions that is effected by UPC. Instead, the technical processes involved in stop and start, in terms of ordering the packets of information and their

transmission, and their analysis by deep package inspection is not the modification or selection of any information. Tacking on an advertisement to a transmission, or modifying it so that some of it is lost, as opposed to being transmitted slowly, would disable the mere conduit defence.

109. The Article does not affect the possibility for a court to require an internet provide to "terminate" or "prevent" an infringement. This language is in marked contrast to s. 40(4) of the Copyright and Related Rights Acts 2000 which refers to the "removal of infringing material". At the start of the Directive, various recitals referred to the objectives to be attained by the Directive. These include, in recital 9, free access to information, in recital 41, balance, and in recital 46 the disabling of access to the information concerned. Recitals 42, 43, 44 and 45 confirm the view which I have given. These provide:-

> "(42) The exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.
>
> (43) A service provider can benefit from the exemptions for "mere conduit" and for "caching" when he is in no way involved with the information transmitted; this requires among other things that he does not modify the information that he transmits; this requirement does not cover manipulations of a technical nature which take place in the course of the transmission as they do not alter the integrity of the information contained in the transmission.
>
> (44) A service provider who deliberately collaborates with one of the recipients of his service in order to undertake illegal acts goes beyond the activities of "mere conduit" or "caching" and as a result cannot benefit from the liability exemptions established for these activities.
>
> (45) The limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds; such injunctions can in particular consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it."

110. Whether UPC is a mere conduit of copyright infringement or not, recital 45 does not remove the possibility of injunctive relief as a matter of European law. The wording, again, bears out the very limited nature of the remedy available in the Act of 2000. The Directive refers to an injunction that mandates "orders by courts… requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it". Each of these concepts, of removal, of termination, of prevention and of disabling are separate. Only one of them, which is that of removal, is referred to in s. 40(4) of the Copyright and Related Rights Acts 2000. The construction of this Directive, therefore, undermines, rather than furthers, the argument made on behalf of the recording companies.

111. The Copyright Directive does not bring the matter further. Article 2 of the directive is mirrored in national legislation in providing for reproduction rights to be vested in the creator of original work, or in the person licensed in that regard. Exceptions and limitations are set out in Article 5, including the scholar's exception, quotations for the purpose of criticism or review, and reproductions, such as music score reproductions, where the right holders receive fair compensation. Recital 16 declares the purpose of the Directive, in part to be:-

> "(16) Liability for activities in the network environment concerns not only copyright and related rights but also other areas, such as defamation, misleading advertising, or infringement of trademarks, and is addressed horizontally in Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market ("Directive on electronic commerce")(4), which clarifies and harmonises various legal issues relating to information society services including electronic commerce. This Directive should be implemented within a timescale similar to that for the implementation of the Directive on electronic commerce, since that Directive provides a harmonised framework of principles and provisions relevant inter alia to important parts of this Directive. This Directive is without prejudice to provisions relating to liability in that Directive."

112. Recital 27 further indicates that the purpose of the Directive is to ensure that the mere provision of physical facilities for copyright infringement is not to be equated with a breach of copyright, save in particular circumstances. Those circumstances are provided for in Irish law by s. 40(4) of the Copyright and Related Act 2000.

113. Recital 59 contains a declaration that, in the light of the evidence in this case, can be seen as a truism:-

> "(59) In the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities. In many cases such intermediaries are best placed to bring such infringing activities to an end. Therefore, without prejudice to any other sanctions and remedies available, rightholders should have the possibility of applying for an injunction against an intermediary who carries a third party's infringement of a protected work or other subject-matter in a network. This possibility should be available even where the acts carried out by the intermediary are exempted under Article 5. The conditions and modalities relating to such injunctions should be left to the national law of the Member States."

114. This recital indicates that the purpose of the Directive is to ensure that injunctive relief is available in national legislation against an intermediary that carries a copyright infringement, even where they are exempted. The relevant exemption here is Article 5.1 of the Directive:-

> "Exceptions and limitations
>
> 1. Temporary acts of reproduction referred to in Article 2, which are transient or incidental [and] an integral and essential part of a technological process and whose sole purpose is to enable:
>
> (a) a transmission in a network between third parties by an intermediary, or
>
> (b) a lawful use of a work or other subject-matter to be made, and which have no independent economic significance, shall be exempted from the reproduction right provided for in Article 2.

2. Member States may provide for exceptions or limitations to the reproduction right provided for in Article 2 in the following cases:

(a) in respect of reproductions on paper or any similar medium, effected by the use of any kind of photographic technique or by some other process having similar effects, with the exception of sheet music, provided that the rightholders receive fair compensation;

(b) in respect of reproductions on any medium made by a natural person for private use and for ends that are neither directly nor indirectly commercial, on condition that the rightholders receive fair compensation which takes account of the application or non-application of technological measures referred to in Article 6 to the work or subject-matter concerned;

(c) in respect of specific acts of reproduction made by publicly accessible libraries, educational establishments or museums, or by archives, which are not for direct or indirect economic or commercial advantage;

(d) in respect of ephemeral recordings of works made by broadcasting organisations by means of their own facilities and for their own broadcasts; the preservation of these recordings in official archives may, on the grounds of their exceptional documentary character, be permitted;

(e) in respect of reproductions of broadcasts made by social institutions pursuing non-commercial purposes, such as hospitals or prisons, on condition that the rightholders receive fair compensation.

3. Member States may provide for exceptions or limitations to the rights provided for in Articles 2 and 3 in the following cases:

(a) use for the sole purpose of illustration for teaching or scientific research, as long as the source, including the author's name, is indicated, unless this turns out to be impossible and to the extent justified by the non-commercial purpose to be achieved;

(b) uses, for the benefit of people with a disability, which are directly related to the disability and of a non-commercial nature, to the extent required by the specific disability;

(c) reproduction by the press, communication to the public or making available of published articles on current economic, political or religious topics or of broadcast works or other subject-matter of the same character, in cases where such use is not expressly reserved, and as long as the source, including the author's name, is indicated, or use of works or other subject-matter in connection with the reporting of current events, to the extent justified by the informatory purpose and as long as the source, including the author's name, is indicated, unless this turns out to be impossible;

(d) quotations for purposes such as criticism or review, provided that they relate to a work or other subject-matter which has already been lawfully made available to the public, that, unless this turns out to be impossible, the source, including the author's name, is indicated, and that their use is in accordance with fair practice, and to the extent required by the specific purpose;

(e) use for the purposes of public security or to ensure the proper performance or reporting of administrative, parliamentary or judicial proceedings;

(f) use of political speeches as well as extracts of public lectures or similar works or subject-matter to the extent justified by the informatory purpose and provided that the source, including the author's name, is indicated, except where this turns out to be impossible;

(g) use during religious celebrations or official celebrations organised by a public authority;

(h) use of works, such as works of architecture or sculpture, made to be located permanently in public places;

(i) incidental inclusion of a work or other subject-matter in other material;

(j) use for the purpose of advertising the public exhibition or sale of artistic works, to the extent necessary to promote the event, excluding any other commercial use;

(k) use for the purpose of caricature, parody or pastiche;

(l) use in connection with the demonstration or repair of equipment;

(m) use of an artistic work in the form of a building or a drawing or plan of a building for the purposes of reconstructing the building;

(n) use by communication or making available, for the purpose of research or private study, to individual members of the public by dedicated terminals on the premises of establishments referred to in paragraph 2(c) of works and other subject-matter not subject to purchase or licensing terms which are contained in their collections;

(o) use in certain other cases of minor importance where exceptions or limitations already exist under national law, provided that they only concern analogue uses and do not affect the free circulation of goods and services within the Community, without prejudice to the other exceptions and limitations contained in this Article.

4. Where the Member States may provide for an exception or limitation to the right of reproduction pursuant to paragraphs 2 and 3, they may provide similarly for an exception or limitation to the right of distribution as referred to in Article 4 to the extent justified by the purpose of the authorised act of reproduction.

5. The exceptions and limitations provided for in paragraphs 1, 2, 3 and 4 shall only be applied in certain special cases which do not conflict with a normal exploitation of the work or other subject-matter and do not unreasonably prejudice the legitimate interests of the rightholder."

115. It is clear, however, that the purpose of the Directive was to ensure that injunctive relief should be available in national law despite an exemption applying as just quoted. Article 8 deals with sanctions and remedies. This provides:-

"1. Member States shall provide appropriate sanctions and remedies in respect of infringements of the rights and obligations set out in this Directive and shall take all the measures necessary to ensure that those sanctions and remedies are applied. The sanctions thus provided for shall be effective, proportionate and dissuasive.

2. Each Member State shall take the measures necessary to ensure that rightholders whose interests are affected by an infringing activity carried out on its territory can bring an action for damages and/or apply for an injunction and, where appropriate, for the seizure of infringing material as well as of devices, products or components referred to in Article 6(2).

3. Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right."

116. Particular emphasis is laid on the obligation cast on the State through the Copyright Directive to ensure that copyright holders are in a position to apply for an injunction against an internet service provider which is being used to infringe copyright. As is made clear, however, by recital 59, the "conditions and modalities relating to such injunctions" are left to the national law of the Member States. There is therefore nothing in the Directive which requires any reconstruction of ambiguity in s. 40(4) of the Copyright and Related Acts 2000 which might enable the Court to implement, in the absence of national law, injunctive relief not simply to presently remove infringing material from an internet site but, in the wording of the E-Commerce Directive, to terminate or prevent a transmission, or to disable access to files being illegally held by customers of UPC as an internet service provider. The implementation of the defences for mere conduit caching and hosting provided in national form by The European Communities (Directive 2000/31/EC) Regulations 2003, do not change this. Nor does the slight alteration in wording contained in Regulation 16(3) thereof in relation to the defence of merely being conduit. Perhaps that difference in wording was thought in the mind of the drafter to be explained by the existence of s.40(4) of the Copyright and Related Act 2000. Whether that is so, or is not so, does not add to the construction of that subsection within its appropriate context.

117. Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) regulates the modalities of approach. The Court notes that Article 1 of the 2002 Directive is altered by Article 1 of 2009 Framework Directive requiring due process and a judicial hearing before internet access is terminated. This directive must be transposed into Irish law, under Article 5, by the 26th May 2011. As of the present time, Article 8.4 provides:-

"4. The national regulatory authorities shall promote the interests of the citizens of the European Union by inter alia:
(a) ensuring all citizens have access to a universal service specified in Directive 2002/22/EC (Universal Service Directive);

(b) ensuring a high level of protection for consumers in their dealings with suppliers, in particular by ensuring the availability of simple and inexpensive dispute resolution procedures carried out by a body that is independent of the parties involved;

(c) contributing to ensuring a high level of protection of personal data and privacy;

(d) promoting the provision of clear information, in particular requiring transparency of tariffs and conditions for using publicly available electronic communications services;

(e) addressing the needs of specific social groups, in particular disabled users; and

(f) ensuring that the integrity and security of public communications networks are maintained."

Article 1, as amended in the future in 2011, will read as follows:-

"1. This Directive establishes a harmonised framework for the regulation of electronic communications services, electronic communications networks, associated facilities and associated services, and certain aspects of terminal equipment to facilitate access for disabled users. It lays down tasks of national regulatory authorities and establishes a set of procedures to ensure the harmonised application of the regulatory framework throughout the Community

2. This Directive as well as the Specific Directives are without prejudice to the obligations imposed by national law in accordance with Community law or by Community law in respect of services provided using electronic communications networks and services.

3. This Directive as well as the Specific Directives are without prejudice to measures taken at Community or national level, in compliance with Community law, to pursue general interest objectives, in particular relating to content regulation and audio-visual policy.

3a. Measures taken by Member States regarding end-users access to, or use of, service and applications through electronic communications networks shall resepct the fundamental rights and freedoms of natural persons, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and general principles of Community law.

Any of these measures regarding end-users' access to, or use of, services and applications through electronic communications networks liable to restrict those fundamental rights or freedoms may only be imposed if they are appropriate, proportionate and necessary within a democratic society, and their implementation shall be subject to adequate procedural safeguards in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms and with general principles of Community law, including effective judicial protection and due process. Accordingly, these measures may only be taken with due respect for the principle of the presumption of innocence and the right to privacy. A prior, fair and impartial procedure shall be guaranteed, including the right to be heard of the person or persons concerned, subject to the need for appropriate conditions and

procedural arrangements in duly substantiated cases of urgency in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms. The right to effective and timely judicial review shall be guaranteed.'

4. This Directive and the Specific Directives are without prejudice to the provisions of Directive 1999/5/EC.

118. The Communication Regulations Act 2002 ("the Act of 2002"), as amended by the Communications Regulation (Amendment) Act 2007, allows for an independent body to carry out investigations, under s. 10(1), into matters relating to the supply of and access to, electronic communications services. This does not imply, to my mind, the resolution of disputes. Indeed, ComReg, the independent body established under the Act of 2002, is neither obligated to investigate complaints nor to resolve disputes involving consumers and operators/internet service providers. These powers there contained are in marked contrast with those provided, for example, under the Central Bank and Financial Services Authority of Ireland Act 2004 ("the Act of 2004"), which amends the Central Bank Act 1942 and which establishes the Office of the Financial Services Ombudsman. More specifically, that Act establishes a clear dispute resolution process, providing the Ombudsman with extensive powers of investigation and resolution. Importantly section 57BY of the Central Bank Act 1942 ("the Act of 1942"), as inserted by s. 16 of the Act of 2004, provides that the Financial Services Ombudsman *shall* investigate a complaint that falls within the jurisdiction of the office. Section 57BY(1) reads as follows:-

> "(1) The Financial Services Ombudsman shall investigate a complaint if satisfied that the complaint is within the jurisdiction of the Financial Services Ombudsman.

The Ombudsman's role is not, however, confined to a mere investigatory one. Section 57CA of the Act of 1942, provides that the Ombudsman must first seek to deal with the complaint by mediation. Failing this, section 57(CA)(4)(a) empowers the Ombudsman to "deal with the complaint by adjudication…" Any subsequent decision of the Ombudsman does not lack bite and will be enforced by the Circuit Court under s. 57CJ where the Court is satisfied that the order made by the Ombudsman was intra vires. In addition, in order to confirm my view, I have looked at how in other European jurisdictions, national measures apply to blocking internet access, or interrupting or diverting transmission, as well as to the removal of material on the internet. I now briefly refer to some relevant examples.

National Measures in Other States

119. Section 3 of the Digital Economy Act 2010 of the United Kingdom inserts a new section into the Communication Acts 2003. In its detailed terms, this provides for a code of practice in relation to the interruption of piracy transmissions. The appropriate modalities are decided upon and overseen by the Commission for Communications Regulations. I therefore quote:-

> "(1) This section applies if it appears to a copyright owner that–
>
> (a) a subscriber to an internet access service has infringed the owner's copyright by means of the service; or
>
> (b) a subscriber to an internet access service has allowed another person to use the service, and that other person has infringed the owner's copyright by means of the service.
>
> (2) The owner may make a copyright infringement report to the internet service provider who provided the internet access service if a code in force under section 124C or 124D (an "initial obligations code") allows the owner to do so.
>
> (3) A "copyright infringement report" is a report that
>
> (a) states that there appears to have been an infringement of the owner´s copyright;
>
> (b) includes a description of the apparent infringement;
>
> (c) includes evidence of the apparent infringement that shows the subscriber´s IP address and the time at which the evidence was gathered;
>
> (d) is sent to the internet service provider within the period of 1 month beginning with the day on which the evidence was gathered; and
>
> (e) complies with any other requirement of the initial obligations code.
>
> (4) An internet service provider who receives a copyright infringement report must notify the subscriber of the report if the initial obligations code requires the provider to do so.
>
> (5) A notification under subsection (4) must be sent to the subscriber within the period of 1 month."

120. Similarly, s. 124(g) provides for a technical solution whereby a subscriber may be prevented from using the internet. The detail of these provisions contrast markedly with their absence in our national legislation:-

> "(1) The Secretary of State may direct OFCOM to
>
> (a) assess whether one or more technical obligations should be imposed on internet service providers;
>
> (b) take steps to prepare for the obligations;
>
> (c) provide a report on the assessment or steps to the Secretary of State.
>
> (2) A "technical obligation", in relation to an internet service provider, is an obligation for the provider to take a technical measure against some or all relevant subscribers to its service for the purpose of preventing or reducing infringement of copyright by means of the internet.
>
> (3) A "technical measure" is a measure that
>
> (a) limits the speed or other capacity of the service provided to a subscriber;
>
> (b) prevents a subscriber from using the service to gain access to particular material, or limits such use;

(c) suspends the service provided to a subscriber; or

(d) limits the service provided to a subscriber in another way.

(4) A subscriber to an internet access service is "relevant" if the subscriber is a relevant subscriber, within the meaning of section 124B(3), in relation to the provider of the service and one or more copyright owners.

(5) The assessment and steps that the Secretary of State may direct OFCOM to carry out or take under subsection (1) include, in particular–

(a) consultation of copyright owners, internet service providers, subscribers or any other person;

(b) an assessment of the likely efficacy of a technical measure in relation to a particular type of internet access service; and

(c) steps to prepare a proposed technical obligations code.

(6) Internet service providers and copyright owners must give OFCOM any assistance that OFCOM reasonably require for the purposes of complying with any direction under this section.

(7) The Secretary of State must lay before Parliament any direction under this section.

(8) OFCOM must publish every report under this section–

(a) as soon as practicable after they send it to the Secretary of State, and

(b) in such manner as they consider appropriate for bringing it to the attention of persons who, in their opinion, are likely to have an interest in it.

(9) OFCOM may exclude information from a report when it is published under subsection (8) if they consider that it is information that they could refuse to disclose in response to a request under the Freedom of Information Act 2000."

121. Finally, there is power to use a blocking injunction, whereby sites such as Pirate Bay, may be prevented from being accessed through an internet service provider. This provided is for in s.17 of the Digital Economy Act 2010:-

"(1) The Secretary of State may by regulations make provision about the granting by a court of a blocking injunction in respect of a location on the internet which the court is satisfied has been, is being or is likely to be used for or in connection with an activity that infringes copyright.

(2) "Blocking injunction" means an injunction that requires a service provider to prevent its service being used to gain access to the location.

(3) The Secretary of State may not make regulations under this section unless satisfied that

(a) the use of the internet for activities that infringe copyright is having a serious adverse effect on businesses or consumers,

(b) making the regulations is a proportionate way to address that effect, and

(c) making the regulations would not prejudice national security or the prevention or detection of crime.

(4) The regulations must provide that a court may not grant an injunction unless satisfied that the location is
(a) a location from which a substantial amount of material has been, is being or is likely to be obtained in infringement of copyright,

(b) a location at which a substantial amount of material has been, is being or is likely to be made available in infringement of copyright, or

(c) a location which has been, is being or is likely to be used to facilitate access to a location within paragraph (a) or (b).

(5) The regulations must provide that, in determining whether to grant an injunction, the court must take account of–
(a) any evidence presented of steps taken by the service provider, or by an operator of the location, to prevent infringement of copyright in the qualifying material,

(b) any evidence presented of steps taken by the copyright owner, or by a licensee of copyright in the qualifying material, to facilitate lawful access to the qualifying material,

(c) any representations made by a Minister of the Crown,

(d) whether the injunction would be likely to have a disproportionate effect on any person´s legitimate interests, and

(e) the importance of freedom of expression.

(6) The regulations must provide that a court may not grant an injunction unless notice of the application for the injunction has been given, in such form and by such means as is specified in the regulations, to
(a) the service provider, and

(b) operators of the location.

(7) The regulations may, in particular–

(a) make provision about when a location is, or is not, to be treated as being used to facilitate access to another location,

(b) provide that notice of an application for an injunction may be given to operators of a location by being published in accordance with the regulations,

(c) provide that a court may not make an order for costs against the service provider,

(d) make different provision for different purposes, and

(e) make incidental, supplementary, consequential, transitional, transitory or saving provision.

(8) The regulations may–

(a) modify Chapter 6 of Part 1 of the Copyright, Designs and Patents Act 1988, and

(b) make consequential provision modifying Acts and subordinate legislation.

(9) Regulations under this section may not include provision in respect of proceedings before a court in England and Wales without the consent of the Lord Chancellor.

(10) Regulations under this section must be made by statutory instrument.

(11) A statutory instrument containing regulations under this section may not be made unless–

(a) the Secretary of State has complied with section 18, and

(b) a draft of the instrument has been laid before and approved by a resolution of each House of Parliament.

(12) In this section

- "copyright owner" has the same meaning as in Part 1 of the Copyright, Designs and Patents Act 1988;
- "Minister of the Crown" has the same meaning as in the Ministers of the Crown Act 1975;
- "modify" includes amend, repeal or revoke;
- "operator", in relation to a location on the internet, means a person who has editorial control over material available at the location;
- "qualifying material", in relation to an injunction, means the material taken into account by the court for the purposes of provision made under subsection (4);
- "service provider" has the same meaning as in section 97A of the Copyright, Designs and Patents Act 1988;
- "subordinate legislation" has the same meaning as in the Interpretation Act 1978.

(13) In the application of this section to Scotland

- "costs" means expenses;
- "injunction" means interdict."

122. There is nothing like these provisions in Ireland. I turn now to France. On the 12 May, 2009, the French National Assembly passed the *'Haute Autorité pour la Diffusion des Oeuvres et la Protection des droits sur Internet'* (HADOPI) law *"Loi favorisant la diffusion et la protection de la création sur Internet"*. This adopted version included important changes to the original HADOPI law which was rejected by the Constitutional Court of France ("the Conseil Constitutionnel"). This rejected version sought to establish in French law a 'graduated-response' approach to tackling online copyright piracy. In its original form the system established a 'three-strikes' policy, with the third strike (the termination of internet access) at the discretion of a newly established administrative body (HADOPI). The empowering of this non-judicial body was struck down as an unacceptable encroachment on the presumption of innocence. In this jurisdiction, that concept would apply only to an accusation of crime. The revised version acknowledges these objections and provides that a court hearing must precede any removal of a subscriber's internet access. HADOPI, this new regulatory body, will investigate alleged breaches of copyright law and recommend appropriate sanctions. Where the body advises that a subscriber be cut-off the judicial arm of the State will be called into action, thereby ensuring that the presumption of innocence and the right to freedom of expression are protected. HADOPI was finally established on the 27th July, 2010.

123. The law specifically targets peer-to-peer file sharing, the undisputed focal point for illegal activity. The United Kingdom definitions seem to be more comprehensive and the law in that jurisdiction to be practical and workable.

124. In Belgium in 2004, in the case of *Scarlet v. Sabam* the Belgian Society of Authors, Composers and Publishers (Sabam) initiated legal proceedings against the ISP Scarlet (originally *Tiscali, Belgium*), before the Belgian national Court of First Instance in Brussels, arguing that Scarlet should be held responsible for the illegal file-sharing activities of its subscribers conducted over its network. In 2007 the Belgian national Court of First Instance held that Scarlet was liable for copyright infringement and required it to take certain steps to prevent its customers from illegally downloading copyright-protected music by installing software to filter and block peer-to-peer files. Of particular relevance is the fact that the Court accepted the expert evidence and was satisfied that the necessary technology existed to effectively detect and filter infringing materials.

125. On appeal the Belgian Court of Appeal referred the following questions to the European Court of Justice:

a. does European legislation [including articles 8 and 10 of the European Convention of European Rights] allow Member States to authorise a national court to order ISPs to install as a preventive measure a system filtering all electronic

communications passing through their service to identify files containing work which a claimant alleges to enjoy the rights of, and to block the transfer of such files?; and

b. if so, are national courts required to apply the principle of proportionality when asked to rule over the efficacy and dissuasive effect of the requested measure?

126. Although judgment will not be delivered in this case until autumn 2011 it is apparent, given the wording of Article 1 of the Directive 2002/EC/EC, as amended by Framework Directive 2009/140/EC, that any measure that imposes restrictions on end-users' access to, or use of, services may only be imposed "if they are appropriate, proportionate and necessary within a democratic society, and their implementation shall by subject to adequate procedural safeguards in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms and with general principles of Community law…"

127. In addition to the judicial remedies sought by Sabam, the Belgian legislature has recognised the need for reform in this area. Two pieces of legislation are currently being debated by the Belgian legislature. The first, introduced on 17 March 2010, proposes a graduated response approach, similar to the HADOPI law as enacted in France. Although based around the same principles – if you fail to comply following a series of warnings you may have your internet access suspended or even terminated – there are differences between the two.

128. The proposed Belgian law offers subscribers three opportunities to respond to rights holders before they risk the loss of their internet access. The process starts with a warning by e-mail. If this fails to deter the user an administrative fine is imposed. Following these two warnings if the user is determined to flagrantly ignore copyright law the user must attend court where a larger fine, or even restrictions on his or her internet access may be imposed. It is only when all of the above steps have failed that the most serious sanction – the termination of an internet account – can be imposed at the direction of a court. Both the proposed Belgian law and the current French law can be argued to comply with Article 1 of the Directive 2002/EC/EC as amended by Framework Directive 2009/140/EC. Article 1 sets out that the termination of an end-user's internet access (or any limitations imposed upon it) must be done following the resolution of a hearing that adheres to fair procedures as required by the European Convention on Human Rights. There seems to be no reason why the District Court in Ireland could not administer inexpensively either such a system or a system of application for information based on proof of IP addresses and infringement, for the purpose of future prosecution by the recording companies.

Other Jurisdictions

129. The Digital Millennium Copyright Act 2000 ("DMCA") was enacted in the United States of America to "criminalize circumventing copyright-protection technology" and to punish online copyright infringement. In particular the Act makes internet service providers liable for infringing activity on their servers so as to stop illegal file-sharing. An internet service provider is defined in 17 U.S.C. § 512(k) as being either "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user…" In a manner akin to the 'mere conduit' defence under European law § 512(h) gives complete immunity from liability to internet service providers who simply transmit information from user to user without caching. The Act also authorises rights holders to serve a subpoena on the internet service provider, asking it to identify the accused infringer. Liability can be otherwise established, it seems, in U.S. law for participation in tort through a failure to act appropriately. In the U.S. Supreme Court decision in *Metro-Goldwyn-Mayer Studios Inc. et al. v. Grokster, Ltd., et al.* 545 (U.S.) 913 the Court held as follows:-

> "When a widely shared product is used to commit infringement, it may be possible to enforce rights in the protected work effectively against all infringers, so that the only practical alternative is to go against the devices' distributor for secondary liability on a theory of contributory or vicarious infringement. One infringes contributorily by intentionally inducing or encouraging direct infringement, and infringes vicariously by profiting from direct infringement while declining to exercise the right to stop or limit it. Although "[t]he Copyright Act does not expressly render anyone liable for [another's] infringement," *Sony*, 464 U.S., at 434, these secondary liability doctrines emerged from common law principles and are well established in law, *e.g., id.,* at 486. Pp 10-13."

130. Of note from an Irish and European perspective is that fact that a court order is required before an end-user's access to the internet can be interfered with. This reflects, as far as I can understand, the critical importance that the U.S. legislature attaches to the right to internet access, freedom of expression and the presumption of innocence, which may apply in that legal system, I do not know, outside the realm of crime. Obvious parallels can be drawn between the French HADOPI II law, the proposed Belgian law and the Digital Economy Act 2010 in the U.K. In addition, the New Zealand legislature has recently introduced the File-Sharing Bill 2010, in an attempt to address piracy of copyright on the internet.

Injunction to Disable Internet Piracy

131. The detail provided for in the legislation briefly referred to providing a remedy against hosting, allowing for a three strikes policy and the disablement of a transmission involving copyright theft over the internet, convinces the Court of the absence of similar provisions in Irish Law. In particular the paucity of the remedy available under s. 40(4) of the Copyright and Related Rights Act is unambiguous. Legislative intervention is required, if the Oireachtas see fit, to protect constitutional rights to copyright and foster the national resource of creativity. The power to block access to internet sites, to disable access, to interrupt a transmission, to divert a transmission, and to cut off internet access in controlled circumstances are amply and clearly provided for in the law of the neighbouring Kingdom and are specifically outlined in the law of other European states and are also highly developed in United States of America law. They are not now available in Irish Law

132. It follows, from the analysis just conducted, that blocking and diverting mechanisms, as opposed to any removal mechanism, such as in relation to hosting are not available under s. 40(4) of the Act.

Pirate Bay Injunction

133. In the second paragraph of their prayer for relief, the recording companies ask for a blocking injunction against Pirate Bay. This site is responsible for the great bulk of internet piracy in this country. Mr. Kavanagh, as I have said, described how he used it. To begin legally downloading copyright material, all that one needs to do is to access Pirate Bay, download the appropriate software from them, search on their website what swarms are active and what tracks are being offered, and then join one of those swarms using the relevant software. Regrettably on a full consideration of this matter, a blocking injunction is not available in Irish law.

134. Were it available, I would grant it. Mr. Harrison, in evidence on behalf of UPC indicated, how, through Eircom, when that access was blocked, he readily found a way through. However, this took him twenty minutes. Professor Nixon offered the opinion that such blocking was futile. I do not agree. In the telecommunications industry it has been noted that where an area moves from access to other areas, such as the Aran Islands to Dublin, or the Aran Islands to New York, by dialling the operator, to direct dial, that the improvement in service causes a leap in usage. This is known as the service improvement jump. It must work in the opposite situation.

I would regard it as both educative and helpful to block Pirate Bay were I enabled by the relevant legislation to do so. At the very least, it declares that the activity is illegal. I cannot grant the injunction because I have no legal power to do so.

Prior Judgments

135. There were two prior judgments of the Court in relation to issues related to this case. In *EMI Records (Ireland) Limited v. Eircom Limited* [2010] IEHC 108, (Unreported, High Court, Charleton J., 16th April, 2010), as has been previously stated, a similar action had been brought against Eircom, as the largest internet service provider in the State. This was settled on the basis of a three strike policy that is fully set out in that judgment. That was a private matter between the parties as a matter of contract. The settlement was not authorised or ruled on by the Court. The Court had no function in that regard. The Court was, some months after the settlement, asked to determine the compatibility of aspects of that settlement with the Data Protection Acts 1988-2003, three issues having been raised in correspondence by the Data Protection Commissioner. In the light of the evidence in this case, and the conclusions that the Court has reached, the Court would wish to make it clear that this judgment is unaffected. I have reconsidered it in the light of the evidence and submissions in this case and I am of the view that the judgment is correct.

136. A different conclusion arises in relation to the earlier judgment of the Court in *EMI (Ireland) Limited v. Eircom Plc* [2009] IEHC 411 (Unreported, High Court, Charleton J., 24th July, 2009). That judgment was, as the first paragraph of it indicates, delivered ex-tempore, having heard, as I said, only one side of the case. In settling the litigation just mentioned, *EMI* and *Eircom*, it was agreed by the parties that an application would be brought to block access to 'The Pirate Bay' website on the facilities of Eircom, as an internet service provider. The conclusion I reached in that judgment, that I was entitled as a matter of law, to block access to that site, was arrived at in the absence of argument to the contrary by Eircom. While Eircom did not consent to the judgment, at the same time, they appeared in court and offered no argument against the analysis in favour of the grant of an injunction: this position of not arguing against the injunction, I understand, was part of the terms of the settlement between those parties. Counsel for Eircom was thus constrained into offering no opposition to the argument.

137. Having fully considered the issue of blocking a site as variant as The Pirate Bay, I regret that my previous judgment in the matter was wrong. The legislative basis enabling me to act in that way does not exist in Irish law as it exists in other European jurisdictions. The parties to that case may wish to reapply, or they may be content that The Pirate Bay should be blocked through the channels of Eircom. No order as to costs was made in that case, as the application was uncontested and costs were not sought as a matter of consent.

Conclusion

138. Solutions are available to the problem of internet copyright piracy. It is not surprising that the legislative response laid down in our country in the Copyright and Related Rights Act 2000, at a time when this problem was not perceived to be as threatening to the creative and retail economy as it has become in 2010, has made no proper provision for the blocking, diverting or interrupting of internet communications intent on breaching copyright. In failing to provide legislative provisions for blocking, diverting and interrupting internet copyright theft, Ireland is not yet fully in compliance with its obligations under European law. Instead, the only relevant power that the courts are given is to require an internet hosting service to remove copyright material. Respecting, as it does, the doctrine of separation of powers and the rule of law, the Court cannot move to grant injunctive relief to the recording companies against internet piracy, even though that relief is merited on the facts.

139. The Court thus declines injunctive relief.