

COPYRIGHT PIRACY AND THE INTERNET

Peter Charleton and Conor O'Keeffe

Fordham University, April 29 2011

The fraught issue of copyright piracy and the ease with which Internet service has facilitated universal distribution has been argued to have magnified the previously small issue of illegal copying into an industry-threatening one. Innovation in the products offered by copyright holders through the Internet, and especially in collaboration with Internet service providers, may be one response to the problem, a commercial one, but where Europe stands in terms of law will be the system into which any such response must fit. That stance is uncertain. Freedoms of expression and of communication, together with notions of privacy under Article 8 of the European Convention on Human Rights, have combined with the recognition of a new and previously unregulated space outside national boundaries that is called the Internet. Almost as a matter of ideology, those who inhabit this space want freedom; the siren call of revolution and the foundation of democracy applied to computers. They have a point. In 2011 the first thing that the Mubarak regime in Egypt did in response to revolution was to shut down the Internet and the mobile phone service. In terms of the legitimate exploitation of musical and cinematic endeavour by copyright, however, liberty of the Internet has led to serious commercial issues that impact in turn on the livelihood of the underpaid and troubled workspace of the creative artist. What such people do for us is to illuminate life. They deserve protection. There is a fundamental human right to reasonably exploit the creation of music, literature and drama. Without it, Beethoven had to sell his *Missa Solemnis* to three publishers, not telling any of them about the sale to the others, and Stravinsky was left without an income from the *Rite of Spring*. The economic impact of creative artists is of real consequence since as regards cinema, music and literature all of us are consumers. Therefore, attempts to condense the dispute here to one between the right to receive information and the right to give information are perhaps misplaced. The right to reasonable payment for the enjoyment of creative works must also be valued.¹ In the European Union, creative industry accounts for around €700 billion/\$1,000 billion, or over 2.5%, of GDP on 2003 figures. Are the

Peter Charleton is a judge of the High Court of Ireland. Conor O' Keeffe is a judicial research assistant to the Irish High and Supreme Court.

1. See Advocate General's Opinion in Case C-70/10 *Scarlet Extended v Société belge des auteurs compositeurs et éditeurs (Sabam)*, a French version of the judgment is available at: <http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=EN&Submit=rechercher&numaff=C-70/10> with an English press summary of the judgment, both of which were last accessed on 9th May of this year, available at <http://curia.europa.eu/jcms/upload/docs/application/pdf/2011-04/cp110037en.pdf>.

responses to Internet piracy of legislators and judges to be fashioned around what is fair, or on the basis of the protection of a valuable asset? The tensions between freedom and control are not easily resolved in cyber-space and are even less easily resolvable in litigation. From the point of view of a judge, the attractions of disciplining any response sought in litigation to what the law provides for, and for that alone, may be seen as both honest and the proper reply to increasingly strident calls from two opposing and never-to-be-reconciled camps. Copyright is enshrined in the Constitution of the United States of America, once fair use is made of that right. In European legal systems, Ireland seems unique in recognising copyright as a human right. This gives copyright fundamental importance in both litigation and legislation. In *Phonographic Performance Ireland Limited v. Cody*, [1998] 4 I.R. 504 Keane J. at 511 declared copyright as having a pre-legislative origin and super-legislative effectiveness as part of the unenumerated fundamental rights under 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.

One respects this proclamation. An ordinary judge, however, doing ordinary cases from day-to-day must have precise laws. European legislation through directives must be founded in the domestic law of each state by local legislation. Each such legislature, including Ireland, France and Britain, has responded independently to the need to protect copyright in various ways that depend on what politicians in those countries see as appropriate by way of implementation and by way of additional protection. How can a judge act on statements of principle alone? Where the field of law is not sewn, it can reasonably be argued that a judge may come in on the basis of a constitutional imperative to protect the property rights that properly belong to creative endeavour by planting such seeds as will grow and feed the need to have a vindication of copyright theft. Faced, however, with a well-ploughed field thickly populated by European directives and by national legislation, faced with even an attractive argument that creative rights are being undermined by theft, is not a judge left to wonder: they have given me the rules, they have set out clearly what

they want regulated and how it is to be done, does not this exclude judicial activity even in perhaps unthought of issues? A divergence between the judicial process and legislative scheme can, as Fuller posits, be a route to the failure of any legal system.²

The Problem

It is easy to infringe copyright. From the first legislation governing this issue in Britain and Ireland in 1709 the right to control the copying of one's own original creative work was cast in absolute terms. Exceptions were needed. Of these, the most obvious is the scholars' exception. You can quote and comment on somebody else's work, while acknowledging the source, provided in doing so a substantial portion of the work is not taken.³ I am told by those in the book business that the usual rule of thumb is around 400 words. But the temptation to copy more than that is always there; especially when it comes to cinema and to music. Until recently, copying was not easy and copies were of an off-putting lack of quality. Edison discovered that a needle running on a wax cylinder, later a shellac disc, left a scratch that reflected the sound inputted into a horn attached to it. Later, inventors found that a magnetic impression of sound could be recorded on a wire and then later a tape. It is only twenty five years ago, with the invention of the CD, that copyright theft on an individual scale begins to become a serious problem. A CD uses a series of 0s and 1s to capture music and images and a laser reads this digital encoding at the high speed. It is simple, but complicated. It is easy to copy. Many people in the 1990s made copies of CDs to play on their car cassette players because, aside from the most expensive models, cars were not equipped for playing music on CDs. In those days, the laser reading systems on CD players would be bumped about if put in a car and it took time for technology to overcome that problem. Several of us, I am sure, made copies of CDs that we had bought by putting them on to cassette and then played them in the car as we went along; or gave them to friends for similar purposes. This is all illegal. It was at this time that the record companies began to complain: we are losing sales because people are copying our CDs on to cassette. They were not taken particularly seriously and it is fair to say that the problem was a relatively small one. In the course of the litigation referred to in this paper, the head of the record companies in Ireland said: "o.k., it was a problem for us because people were taking our music and putting it on to cassette. But at least to do that [they] had to buy the CD and that way we got

² See L. Fuller, 'The Morality of Law', (1964) Yale University.

³ See Chapter 6 of the Copyright and Related Rights Act 2000 ("the Act of 2000").

sales". The cases referred to here are *EMI v. Eircom*⁴ (*injunction to disable access to Pirate Bay on hearing only EMI*), *EMI v Eircom* (*approval from data protection point of view of the three strikes and cut-off settlement*) and *EMI v. UPC*⁵ (*refusing any relief on a full hearing*). For any Irish judgment mentioned here see www.courts.ie or www.bailii.org.

Emails, word-processing and the Internet are so ubiquitous now that it is hard to imagine the world without them. Over the course of the last ten years, every eighteen months to two years has seen an improvement in the memory capacity of computers of one hundred percent for the same physical space. Another thing happened with the invention of the Internet and it was this other factor, more than anything else, that has joined up with computer technology and the Internet to fundamentally undermine the legal protections inherent in copyright. Digital recording was necessary for CD technology. People criticised it initially and said that because it was an illusion of ones and zeros turning on and off at the speed of light that it did not really capture the sound of the human voice or of strings or whatever. Despite these objections, there was no stopping digitization. The digital nature of recording means that every copy is perfect. There is some degradation in sound copying from CD on to cassette and the more it goes on the more the sound quality decreases. But a man in Chicago, using the Internet, can send a woman in Moscow a completely perfect copy of a digitally scanned photograph, of a digitally filmed movie or a digital recording. So, now we have the opportunity, unlike CD to cassette, for perfect piracy; facilitated by the Internet.

The next link for this phenomenon was peer-to-peer transmission. The Internet consists of thousands of linked computers. The box that you have in your house for telephone or wired connection contains a number, it may be your telephone number, but if you have a router box it will be a different number. You always keep that router box number but it never appears on Internet communications. Then, from day-to-day you will be assigned an Internet protocol ("IP") number. This will be attached to all of your transmissions on any particular day. Groups of IP numbers are obtained by Internet service providers from an international body in Paris.⁶ From day-to-day only the Internet service providers know what IP number you have been assigned. With every transmission that you make, your IP number will be attached.

4 [2009] IEHC 411, (Unreported, High Court, Charleton J., 24th July, 2009) on the grant of an injunction against the defendant Internet service provider to block access to Pirate Bay, later declared to be incorrect in *EMI v UPC* [2010] IEHC 377, (Unreported, High Court, Charleton J., 10th November, 2010); *EMI v Eircom* [2010] IEHC 108 on data protection upholding the validity of the three strikes and cut-off settlement as between the parties.

5 [2010] IEHC 377, (Unreported, High Court, Charleton J., 10th November, 2010) holding that the grant of an injunction was not possible to require an Internet service provider to implement a three strikes and cut-off policy.

6 Réseaux IP Européen.

Internet service providers are basically the owners of huge computers that ensure that your computer is linked up to theirs and thus to Internet service providers in different parts of the world and then into people's offices, workplaces and homes. These computers are on all the time and transmissions pass through them every second. Sometimes they temporarily store communications for onward transmission or cache frequently used websites. Essentially, however, this can be argued to be part of the transmission process.

The more complex an artwork becomes, the more difficult it is to store on your computer. Simple files involving judgments, for instance, will take up only a small amount of space and are easily put on a memory stick. That is because these are words only. If, however, you attempt to put a video, or to a lesser extent a recording of music, on your average memory stick, it will take up a big chunk of the memory. Peer-to-peer technology was invented to overcome the problems of memory. Essentially, what it does is that it uses huge numbers of computers that are not necessarily linked to the creator or seller of the film or music. When you link into a peer-to-peer network you get a piece of the film, television programme, or piece of music from every other computer that is at that time linked in to the network. Hence, one might imagine that a jumble will arrive. No, instead, each individual piece of a couple of seconds has a file # attached to it that puts it in the right order on your computer so that you can hear the music or see the film. The file # is a digital code. It is a bit like taking apart a building but numbering every brick. That is how peer-to-peer technology works. The computer puts it together at close to the speed of light. This technology is used, for example, by national radio and television broadcasters. This is because they want to have popular programmes available on their websites for people to look at again and again or for those who missed the programme. To host their film or radio transmissions on one computer for thousands or millions of takers would be a gigantic task requiring massive memory. Downloading would also be slow. Downloading becomes fast with peer-to-peer because several people, sometimes thousands or millions, have already stored popular programmes and when they are online you can link in to their computer through peer-to-peer technology and the Internet will select the swiftest route for putting together the complete article on your home computer: a bit from here there and everywhere but put in perfect sequence when it arrives. Peer-to-peer and digital recording, the one inseparable from the other, combined to create a perfect storm of illegal downloading. That system arose from peer-to-peer as a legal application and it is increasingly lawfully used even for the retrieval of office data.

Peer-to-peer technology has been claimed to have had a devastating impact on video and music companies. Anyone going into an appropriate site, the most notorious of which is called 'The PirateBay', can download the technology for peer-to-peer transmission. You can then go into another site which indicates what music is on offer, or what films are on offer, choose a track or a film and start downloading it. Within minutes you can have a CD or DVD that you would have paid €15/\$20 for in a shop or the film that you felt you wanted to buy, but stopped yourself from buying. A few figures are appropriate here in relation to the experience in Ireland, a very small country of about 4.5 million people. When Ireland's economy was experiencing a false high property price boom between 2005 and 2008 (our real economy has actually grown on a sustainable basis and remains very sound outside the banking sector) the music industry experienced a 40% reduction in the sales of recorded music. Why the drop in CD sales? International studies have shown a ratio of 1:0.42 as the number of unauthorised downloader's of music for every broadband Internet line. Since there are one and half million broadband subscribers in Ireland it seems likely, on this ratio, that some 600,000 to 700,000 people will engage in music piracy from time-to-time. This has resulted in at least €2/\$3 million in annual lost sales to the music firms in a very small country. In addition, retail outlets are being hit. An album by the Irish group Aslan, who used to sell around 35,000 copies per album, on their last offering sold only 6,000 copies. When the Internet was looked at, 22,000 copies of this album was available for illegal download! A Chinese friend of mine who lives in Ireland rarely goes to the cinema; she watches each new film for free in her own language on the web as soon as it comes out. In terms of cinema and music consumption, the situation in Europe will differ little from Ireland. The situation for cinema and music companies is publicly presented by them as a disaster for them and the artists that they support. Hence the application for injunctive relief in the cases to which I am referring. Stop the Internet carrying this traffic and you stop copyright theft, was the argument.

The Pattern

The first case was *EMI v. Eircom*. A lot of expert evidence was presented, including people flown in from abroad, one of whom was one of the actual inventors of the Internet. After eight days of evidence the parties settled. Eircom, Ireland's biggest Internet service provider, agreed that they would start operating a three strikes policy. The Court had no involvement in forging this deal, but this is what was publicly announced: the music recording industry would search the Internet, find the IP numbers involved in illegal downloading using a technology called DtecNet, and inform Eircom. Eircom, who alone would know on what day what IP number

was assigned to which customer, would then write to these subscribers giving them a warning. If they didn't heed three warnings, then they would be cut-off. This is called internationally the "Three Strikes Response". The customer subscriber policy of Eircom, and the customer subscriber policy of UPC, the Internet service provider defendant in a later case, officially deprecates copyright piracy and provides for cut-off as a matter of contract for any customer who infringes. The second part of the settlement in the Eircom case was that Eircom would not oppose an injunction to shut down the PirateBay website.⁷ I heard that application. Counsel for Eircom remained completely silent, like a gilded statue in a Chinese temple. Not his fault; that was his client's instruction. I granted the injunction on the basis that European law mandated it. I did not look closely enough, however, at the transmission of the European directives into Irish law. That decision caused an international hullabaloo in cyberspace. It passed over my head. Then one day senior officials from the Courts' Service contacted me. Senior members of An Garda Síochána (Irish police force) wanted to meet with me. I said yes. The next day two impressive Garda superintendents, and two officials from the Courts Service, diminutive figures in comparison, came to my room. Over tea they told me that this judgment had not gone down well in places like Kazakhstan and Uzbekistan, among others; these are places where there is no control at all of the Internet, or so I was told. I was regarded as a traitor, would you mind, to freedom of expression on the Internet. Threats were made that my life would be "wrecked by computer". Ahem! So, how is that done, I asked? The people in question, the cyber-terrorists, were proposing to hack in to my computer to get my credit card and other details, order any number of pizzas for my greedy gut and get call girls to turn up to my door and plant child pornography on my work computers. Viruses as well, of course. Certain precautions were taken, in consequence. One precaution was to put up firewalls. These work so well that my computer is so slow that I have stopped using it. So, they did get their revenge. A precaution that I personally took was to tell senior figures in the judiciary by email that there were threats to me on the Internet. I got a phone call from a very senior person. The following may or may not be exaggeration or fiction in aid of seeming like some kind of a cool dude: "Dear me Peter, are you sure you're not taking this too seriously?" My reply was: "I'm not taking this seriously at all; it is the police that rang me, not the other way around. Furthermore I'm telling you because if anything happens like a pornography scandal on my computer I want an alibi". The response was: "Peter, in that case, I'm happy to be your alibi".

⁷ EMI v Eircom[2009] IEHC 411, (Unreported, High Court, Charleton J., 24th July, 2009) on the grant of an injunction against the defendant Internet service provider to block access to Pirate Bay, later declared to be incorrect in EMI v UPC [2010] IEHC 377, (Unreported, High Court, Charleton J., 10th November, 2010).

In Ireland, we are used to people being passionate about politics and about religion. I had up to then not realised, however, that there were people out there who believed that their place and state was the Internet; who fiercely guarded it and who considered any attack upon its freedoms to be akin to an assault on a nation state. But they are there and they are, from what I am told, dangerous. They have also led to a great deal of contentious thinking on this topic. It is reflected in international debate.

It seems reasonable to propose that you either have copyright protection or you do not. Can it reasonably be said: we'll have copyright protection except on the Internet? It can be argued that if you treat the Internet as being somehow disconnected from laws of privacy, decency and property that its universal use will undermine the legal order. But the advocates of Internet freedom have their spokespersons. I am sure that they are well-meaning people. In consequence, responses in European law to this, which were once straightforward, have now become entangled with issues of privacy, issues of data protection, issues of personal freedom, entitlements to communicate and, ultimately as you will see from the judgment in *EMI v. UPC*, a requirement that will operate from May 2011, that no one is to be cut-off from Internet service unless there is judicial determination⁸. The termination of a contract is thus, arguably for the first time in European law, made subject to prior judicial supervision. Previously, contracts were private and if broken could be sued upon. Now, an Internet service contract is to assume a special and protected status. We, as members of the judiciary, are consequently drawn in to disputes as to abuse of copyright as between Internet service providers and consumers and music and cinema companies. This may be deprecated by some as private law taking on public characteristics, but judges have a job to do. More widely, as part of the fraught debate on freedom of the Internet, judges are likely to be called on to interpret any solution to the general problem of Internet piracy. Therefore I want to turn to and look at the technical solutions that the cinema and music companies propose, and might ask us to approve or accept or make injunction orders on.

Solutions

Solution 1. One solution tried by the cinema and music companies to undermine Internet copyright piracy was to seek orders in accordance with *Norwich Pharmacal v. Custom and Excise*.⁹ In that case, the House of Lords in Britain, now their

⁸ See Article 1 of Directive 2002/EC/EC, as amended by Framework Directive 2009/140/EC

⁹ [1974] A.C. 133. This approach has been followed in other jurisdictions. For example, in the U.S., The Recording Industry Association of America ("RIAA") has also sought to bypass ISPs as a source of

Supreme Court, established that you could issue proceedings against a person who was aware of the identity of, or otherwise had information about, a party that had perpetrated a civil wrong against you. On establishing this, the defendant had to supply the plaintiff with information enabling a separate suit against the party which had wronged the plaintiff. The decision was followed in Ireland, as in many countries sharing the Anglo-American legal system. So, in *EMI Records (Ireland) Ltd . v. Eircom Limited*¹⁰ Kelly J., presiding judge of our commercial division, made a series of orders compelling Eircom to give the IP addresses of people detected through the DtecNet technology by the music companies taking their copyright files on the Internet. The solution apparently perused by this strategy was: give us the names and addresses of the infringers identified by IP number and we will sue them individually and so teach both a particular and general lesson. The problem was that the costs of everyone have to be paid in these civil find-out procedures. There was bitter correspondence between the recording companies and the Internet service provider over this issue. Dozens of lawyers turned up to represent the interests of various parties. For three sets of orders identifying a total of 89 names the legal costs were €600,080/\$1,000,000. The way this solution should work is that when the recording companies have the names and addresses relevant to the infringements of particular tracks on particular days, which can be gotten only from the Internet service providers through the IP address, they then move to sue or prosecute the infringers. Any such action by way of civil suit or criminal summons takes place in public. In those circumstances privacy is infringed, but it is infringed through a judicial order. These procedures authorise a break in to the closed system where only the Internet service provider can know at any time what a customer is up to. When the music company gets the information, “the customer is so and so from such and such an address”, they can sue or prosecute. In Belgium, this has been one of the recent solutions to Internet piracy; but one proposed through legislation, not judicial activism. They had made it cheaper as a response by allowing their local district courts make Norwich Pharmacal type orders, though it is not called that over there. Some evidence on the likely response to such orders was given in the sets of Irish litigation. The 89 people uncovered in Ireland were contacted. Most were householders or business owners who were unaware that their computers were being used in this context: it was, they said, a teenage son or an employee wasting company time. The vast majority were extremely embarrassed. Virtually everyone,

information, applying directly to court. To date, they have initiated in excess of 35,000 proceedings against subscribers and have had some, albeit limited success. As far as I am aware, only two reported cases have gone to a full hearing, one of which involved a 17 year old boy who took a stance, refused to settle, and was duly delivered a \$675,000 bill by an unimpressed jury: See, *Sony BMG Music Entertainment v. Tenenbaum*, No. 1:07-cv-11446-NG, 2009 U.S. Dist. LEXIS 112845. This amount was reduced to \$67,500 on appeal, a still not insignificant amount.

10 [2005] 4.I.R. 148.

except for one or two, agreed to put an end to it immediately. This may be likely to be the more general response to this kind of detection and notification exercise, though it can be argued that we do not yet precisely know. Why should this be so? Some may feel this kind of theft is enhanced by the private nature of Internet use and that when it is exposed to the public gaze people are embarrassed and stop. As a solution it might work but it cannot possibly do so in the context of the level of expense associated with applications in the higher courts in Europe. Perhaps the Belgian solution of leaving the task to local and less expensive courts may be worth looking at?

The only other possible solutions to Internet piracy are technical things and the real issue there is as to whether they work and as to how they interact with law and human rights? There must be two sides to this. On the one hand the consumers of Internet service will assert an entitlement to privacy, to judicial access and to freedom of the Internet. Their advocates will posit that any activity of copyright theft is small scale and that any detection, warning and cut-off or even a diversion solution is disproportionate. On the other hand, business leaders know that a small choice, for instance to buy a particular brand of chocolate bar, if replicated by multiple people on a habitual basis is the very foundation of commerce. It can reasonably be argued, therefore, that individual theft of copyright material, often repeated, by many millions of people is industrial in terms of the scale of the problem and is public in terms of the notice that should be taken of the harm done.¹¹ For a large scale problem, a technical solution presents as a potential response. Does this mean that technical solutions either work or are mandated?

Three Technical Solutions

Three technical solutions were discussed at length in the Irish litigation, with expert evidence from abroad. I want to briefly describe these, because they are likely to come up in either litigation or legislation contexts.

Solution 2. The first of these was CopySense, this is a popular programme in the United States of America and it is produced by Audible Magic. At the moment, I believe that it is only being tested by being used in universities. The reason for its popularity in the United States of America is the Digital Millennium Copyright Act 2000 which, Americans being ahead of Europeans in this respect, required all institutions of higher education to control Internet piracy on their computer

¹¹ This was recognised in R (British Telecom) v Secretary of State for Business, Innovation and Skills [2011] EWHC 1021 (Admin).

networks.¹² Every student in an American university is linked in to the Internet. That operates both as an intranet for scholars and lecturers alone through password authorisation and the wider Internet. From the intranet, the students will obtain class notes, lectures and materials for research. On the Internet, they may be directed to research materials from the course studies. If a student does not have access to the Internet, then her or his career in an American third level institution is finished. Evidence was presented that in the University of Florida it is impossible to pursue any course if you don't have computer access. My daughter has just commenced a science course in Trinity College Dublin, and again, unlike in my day, the Internet is essential to study. If you breach the acceptable use policy of Florida University, you will be subject to cut-off. This applies to both students and academics. Trinity College Dublin has not yet got such a policy.

CopySense acts like an antivirus programme. It has a database of file # signatures, which are basically of thousands of the most popular copyrighted musical tracks. It does not monitor the contents of email or other web-searching. It operates only within the peer-to-peer protocol which the university's scrutiny software identifies and then analyses by deep packet inspection. The programme has been shown to work in a university with 49,000 students and 200 buildings. The size at which it may operate, therefore, is that of a very small Internet service provider in European terms. Privacy can be argued to be involved in all of these solutions. This proposition can also be an attractive trap. The content of the communication is not searched beyond detection that there has been a breach of copyright. That is all that the student is notified of. If she or he wants to dispute that then perhaps a private conversation with the dean of studies needs to explore what happened further. This CopySense response can be argued to be a programme that can be developed further for small and medium-sized Internet service providers. On detection there will be a warning, followed by another warning, followed by a final warning, and then removal from service. The witness who gave evidence in relation to how it worked in Florida University indicated that every student contacted complied because the consequences of not complying were the effective end of the individual's studies. Obviously, Florida University knows what the students are up to and exercises discipline over them on a named basis. The university may be said to be exercising a kind of parental authority; some may argue that this is inappropriate in the wider community. As to whether this threat might apply more widely, may become a matter for judicial decision at some stage. There are arguably some potential privacy implications in this solution.

12 See s. 512, particularly subs. (e), of the Digital Millennium Copyright Act 2000. See also, Berkeley Technology Law Journal, vol. 21, Issue 1 (2006), pp. 558-559.

Solution 3. Global file registry is akin to a system operated by police in Australia in relation to child pornography images. It is a very sensible system in that context and it seems to work well. In Australia the police store about 70,000 images by reference to their file #. Powerful computers operated by the police are used for detection purposes. They link in to widely offered communications and Internet email and search for the file #. That has a privacy implication. Again, this might also operate on the peer-to-peer protocol by deep packet inspection. Moving outside a police application, instead of detection and prosecution, Global file registry in the general Internet piracy of copyright context detects a relevant copyright infringement, immediately stops it, and then diverts it to a legal site. It never seeks to find out, and never does find out, to whom the IP address attached to all such communications is assigned that particular day. There are arguably no privacy implications; all that the customer sees is that her or his attempt to get something free on their computer has been replaced with an offering for a price. Their frustration must be mighty. In any of these types of programmes, by using proxy searching, the intending infringer can get around them. This takes time, trouble and intelligence. In the ordinary way, Global file registry will therefore force the intending infringer on to a site where thousands of tracks are available for legal download at a reasonable fee. The programme hasn't been fully developed and is really only in testing in two Internet service provider networks. At the moment it seems to be capable of being integrated with the relevant machinery for Internet service providers, but it probably needs further testing.

On the issue that for every solution to copyright piracy there is a response, it may be said that a technology war has started between those who foster copyright and those who desire Internet freedom. That war is likely to have many battles. The service technology jump should not be overlooked in any context where to do something simple such as making a phone call or stealing a music track is involved. All of the studies disclose that where communities moved from telephone operator mediated communications to direct dial, or from land line to mobile, the ease of communication greatly increased the frequency of use. Does it follow that where you make theft of copyright more difficult, that you discourage all but the most determined?

Solution 4. It has been widely argued in Europe that the solution most likely to deter Internet copyright theft is that of detection, followed by warning and cut-off. This response, using DtecNet type software, identifies the copyright material through deep packet inspection on peer-to-peer protocols, it takes a note of the date, the time, the song and the parties to the transmission who are downloading and it

captures their IP address for that day. The music companies do this searching and data collection. Having obtained this anonymous information from the music industry doing the searching (remember the IP address is known only to the Internet service provider and changes from day-to-day) the Internet service providers will warn the infringers. This annoys them, no doubt, but it is hard to see that it impacts on their privacy. It is a matter within the contract between the Internet service provider and their customer. In Europe it is widely reported that the Internet service providers are refusing to run detection solutions and refusing to cooperate with or initiate any three-strikes-and-you're-cut-off solution. In the settlement hammered out between the parties in the *EMI v. Eircom* case, Eircom agreed to act on the basis of information supplied by the music industry. Acting apparently on the basis that detection and warning will stop the vast majority of people, it is only on the third or fourth occasion, and after several stern letters and an attempt of education, that cut-off will occur. This happens pursuant to the existing customer-provider contract. The pirate can then take up with another Internet service provider. The solution did not mandate the sharing of information or a national register of those cut-off. There is every indication that at its peak in Ireland there could be in excess of 40,000 illegal downloads per month (remember that it is out of only 1.5 million subscribers). Warning or cutting off that number of subscribers per month was presented in evidence in the *EMI v. UPC* case by the defendant as an impossible administrative burden for the Internet service providers. Does one need, out of 40,000 infringers, however, to proceed to cut-off every one especially as in the sample of 89 quoted earlier for the Norwich Pharmacal order sample all but around 2% embarrassedly agreed to desist? The music industry would respond that they are seeking out the cut-off of the worst infringers. Going back to the Norwich Pharmacal orders and what was discovered there, it emerges on the evidence that most downloaders were occasional. Some, on the other hand, were determined and had up to 30,000 downloaded tracks on their computers. How could anyone listen to all of that? The music and cinema industry argue that these are the ones that need to be found out and dealt with. The rest can wait, they would say. When cut-off from one Internet service provider these people can take up with another. No one suggested in any of the Internet piracy cases in Ireland that there should be a central registry maintained among the Internet service providers or, worse still, that pirates should be identified publicly in the newspapers; which is the way we deal with tax defaulters in Ireland. This would have possibly critical privacy and data protection implications. An interesting aspect of the three strikes detection and warning process is that it is proposed that both sides share the cost. The music industry does the detection, and pays for it, and the private relationship of Internet

service provider and customer is never infringed but that side bears the costs of administration.

The cost implications of such systems and who must bear them, may prove to be difficult, but not insurmountable stumbling blocks. In *R. (British Telecom) v. Secretary of State for Business, Innovation and Skills* the English High Court, while approving the overall scheme of the English legislation, found that the costs system proposed, under which the Internet service providers would be liable for 25% of the regulators costs and also the costs involved in setting up an appeals process was unlawful and amounted to an administrative charge. This finding, however, is not fatal, with a revision of the draft costs order seen as an adequate remedy. The downside may be that the music industry has to take the word of the Internet service providers that they are really warning people and cutting people off. In the settlement of the *EMI v. Eircom* case they produced a concise but elaborate document allowing for checks and controls and exceptions (such as not cutting off the housebound and dealing with commercial entities separately). Part of this, by the way, was that Eircom agreed to engage with EMI in the provision of a new service; pay €10 a month and have unlimited downloads of most of the new music material. This is now up and running, though I have no idea how mutually beneficial it may have proved to be. Maybe that is one of the ways any real solution to this thing is going to go?

Solution 5. I might add that in the first case of *EMI v. Eircom* other solutions involving the Internet providers having automatic recognition of copyright files through deep packet inspection and automatic cut-off of the attempted download. I do not propose to go in to this. These solutions will take time to test. Such a solution is the subject of litigation in *Scarlet Extended v. Société Belge des Auteurs compositeurs et éditeurs (Sabam)* [Case C-70/10].¹³ It has not so far met with the

¹³ Specifically, the questions referred to the ECJ are as follows:-

“Do Directives 2001/29 (1) and 2004/48, (2) in conjunction with Directives 95/46, (3) 2000/31 (4) and 2002/58, (5) construed in particular in the light of Articles 8 and 10 of the European Convention on the Protection of Human Rights and Fundamental Freedoms, permit Member States to authorise a national court, before which substantive proceedings have been brought and on the basis merely of a statutory provision stating that: ‘They [the national courts] may also issue an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right’, to order an Internet Service Provider (ISP) to introduce, for all its customers, in abstracto and as a preventive measure, exclusively at the cost of that ISP and for an unlimited period, a system for filtering all electronic communications, both incoming and outgoing, passing via its services, in particular those involving the use of peer-to-peer software, in order to identify on its network the sharing of electronic files containing a musical, cinematographic or audio-visual work in respect of which the applicant claims to hold rights, and subsequently to block the transfer of such files, either at the point at which they are requested or at which they are sent?

2. If the answer to the question in paragraph 1 is in the affirmative, do those directives require a national court, called upon to give a ruling on an application for an injunction against an intermediary whose services are used by a third party to infringe a copyright, to apply the

approval of the Advocate General in his advice to the European Court¹⁴. Those of a sceptical frame of mind might posit that these technical solutions would be more advanced as to testing and application were there money in them for the Internet companies. I have no view. In addition, and more importantly, it was mooted in litigation that peer-to-peer communications using particular software should be cut-off or strangled. No decision was made on this idea but it requires to be looked at in brief.

Authorisation

It must be born in mind that the more a technology is used for a lawful purpose, or even can be so used, the less likely that it will be attacked by any order of a court in inter-parties litigation. This was the experience of litigation in the pre-Internet era under the rubric that was then fashionable of ‘authorisation of a breach of copyright’. Twin tape recorders, allowing the copying of one cassette tape onto another, did not amount to authorisation in *CBS Songs Ltd. v. Amstrad Consumer Electronics Ltd.*¹⁵ The House of Lords rejected an argument that by making and selling the tape recorders which allowed people to make illegal copies that there had been the authorisation of multiple breeches of copyright. Dismissing this argument, Lord Templeman doubted the Australian decision of *Moorehouse v. University of New South Wales*¹⁶ which was to the effect that failing to warn against the illegal use of a photocopier in a library and failing to supervise its use amounted to authorisation. Instead, he approved Lord Justice Atkin’s dictum in *Falcon v. Famous Players’ Film Co*¹⁷ that authorisation means the grant or purported grant, which may be expressed or implied, of the right to do the act complained of. Since the manufacture and sale of twin cassette machines did not authorise, but merely empowered, infringing behaviour no injunction would be granted. They could equally be used for a legitimate purpose. Their advertising did not authorise, incite or encourage any breach of copyright even though there was no doubt that it happened.

Authorisation and encouragement of copyright infringement in a peer-to-peer context have been considered in the recent decision of the Full Court of the Federal

principle of proportionality when deciding on the effectiveness and dissuasive effect of the measure sought?”

¹⁴ See Advocate General’s Opinion in Case C-70/10 *Scarlet Extended v. Société belge des auteurs compositeurs et éditeurs (Sabam)*, a French version of the judgment is available at:

<http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=EN&Submit=rechercher&numaff=C-70/10> with an English press summary of the Opinion, both of which were last accessed on 9th May of this year, available at <http://curia.europa.eu/jcms/upload/docs/application/pdf/2011-04/cp110037en.pdf>.

¹⁵ [1988] A.C. 1013.

¹⁶ [1976] R.P.C. 151, doubted and not followed in Canada in *Law Society of Upper Canada v. CCH Ltd.* [2004] F.S.R. 871.

¹⁷ [1926] 2 K.B. 474. I wish to record that my understanding of these issues has been assisted by discussions with Lord Justice Dónal Deeny and Clare Archbold of the Northern Ireland courts.

Court of Australia. In *Roadshow Films Pty Limited v. iiNet Limited* the Court upheld the findings of Chowdry J., sitting as a sole Federal Court of Appeal judge, that the defendant Internet service providers had neither authorised nor encouraged copyright theft by advertising the ease with which its services could be used to download music and/or videos.¹⁸ Choking peer-to-peer communications, or blocking transmissions using particular protocols that use that system, may prove not be attractive to the judicial mind for similar reasons.

Other Countries

The United States, the United Kingdom¹⁹, New Zealand²⁰, Belgium and France are proposing their own solutions in terms of copyright protection for Internet piracy. The French constitutional court has insisted on judicial intervention before anyone is cut-off from Internet service.²¹ That may be fair enough, I do not know. It seems to me that there are generally no privacy implications in someone being cut-off from Internet service where all that is happening is that they are cut-off from one provider, and then can go and annoy another somewhere else.

Privacy

A lot of emphasis was placed during the course of the Irish litigation on privacy rights. Privacy is easy to define as the right to be left alone, but declaring when that right arises is a matter for judgment. Every situation of privacy is dependant on circumstances. One expects privacy, for instance, between husband and wife in their marital bed. Totalitarian regimes expect to be able to interfere even there. With the collapse the German Democratic Republic and the opening of the Stasi files, many people awoke with horror on reading that their spouse had been informing the authorities as to their political views. The attitude involved in such gross infringement of the traditional realms of privacy is the stuff of George Orwell's '1984'; it would not accord with the history and traditions of the United States of America or of Ireland or any other democratic nation. On the other hand, no reasonable person expects privacy on the sidewalk of 5th Avenue or of Unter den Linden. Even in public, you may assert a privacy right by whispering in a friend's ear or even quietly taking someone aside for a chat. All of this is desirable and lawful. Privacy asserts itself both in private situations as they are ordinarily recognised by sensible people and in circumstances where privacy should

¹⁸ [2011] FCAFC 23. See in particular, paras. 626 and Part C of the judgment of the Court.

¹⁹ See The Digital Economy Act 2010, discussed in greater detail below.

²⁰ See the New Zealand Copyright (Infringing File Sharing) Amendment Act 2011, which comes into force on 1 September 2011.

legitimately be protected. The legitimacy of the communication must also be an aspect of whether privacy should be recognised at all. If a man places a bet with a bookie, is this private? Is the strength of any argument in favour of the notion that a man's hobbies, even a man's vices, are essentially a private matter undermined if telephone betting is made illegal? If a man rings up another man and arranges to kill a justice of the peace, they may expect privacy but they must surely lack any basis of entitlement. The legitimate assertion of rights of privacy clearly must depend on what you are doing and how you act in apparent assumption of confidentiality and for what purpose. There is a Grimm's fairytale in which Hans and Kate go on a trip. Kate is stupid and her husband boneheaded. On her journey she falls in with robbers and they ask her to go into a village and steal. She is so honest, however, that what she does is stand out in the middle of the market place, open her arms and say "my dear people can you tell me please what have you got for me to steal?" Is peer-to-peer communication for copyright theft comparable? I have heard it asserted that everyone who goes on this traffic enters it on the basis of stealing material from whoever else joins a swarm with them and allows their own computers to be invaded and downloaded in respect of material. The relevant peer-to-peer protocol available from the PirateBay website makes this automatic, it is said. It makes the communications multiple and solely for the purpose of theft. Can this legitimately be classified as a private activity? Well Advocate General Cruz Vilallón certainly thinks so as he has declared in his opinion for the European Court in *Scarlet Extended* that there is a right to remain anonymous in cyberspace.²² He said: "*D'une manière générale, comme la Commission l'a parfois constaté, la possibilité de rester anonyme est essentielle si l'on veut préserver les droits fondamentaux à la vie privée dans le cyberspace.*"²³ As Professor Hugh Hansen pertinently observed at the 2011 Fordham Intellectual Property Conference, it is difficult to see that right to anonymity applying to child pornography transmissions or other vile crimes. I think that this is correct. A right to privacy in communication cannot sensibly be argued to apply to the arrangement of vicious crimes. But, does a right of privacy inure to arguably small and expectedly private, though admittedly illegal, arrangements? What if the illegalities are apparently petty but are so often repeated and by multiples of offenders that public rights are affected? Some may have great difficulty with any rights to privacy applying to protect criminal activity. I wonder what views might be eventually accepted and the judgment of the European Court is awaited with great interest. Any view that I expressed judicially, in any event, was based on the state of the evidence before me. In the *EMI v. Eircom* and *EMI v. UPC* litigation no one was saying that peer-to-peer copyright theft was a

²² *Scarlet Extended v. Société Belge des Auteurs compositeurs et éditeurs (Sabam)* [Case C-70/10].

²³ *Ibid* at para. 71.

private activity. In fact, the computer experts on both sides were saying precisely the opposite; but that is only their point of view.

Limits

When it came to the trial of the issues between EMI and UPC in *EMI v. UPC*, unlike the issues between EMI and Eircom that were settled in *EMI v Eircom*, everything was litigated. The case went all the way to the end. EMI sought an injunction to prevent the use of the Internet to steal copyright. UPC said it was a mere conduit, thus exempt from damages in European law; that any injunction requiring three strikes and cut-off solution would be a severe burden; that they had no awareness of copyright piracy using the Internet; that the proposed detection, diversion, or disconnection machinery was not properly developed or tested and should not be imposed by injunction; and that the Court should exercise its discretion in equity against granting an injunction. I cannot properly make any comment on these arguments beyond what was in the written judgment. An exploration of the law in general is possible, however. The only authority of the Irish High Court to act to prevent copyright piracy through the medium of the Internet is contained in s.40(4), of the Irish Copyright Act. I now quote sections 40(1), 40(2), 40(3), and 40(4):

40(1) References 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,*

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.”

- (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.*

What does the requirement mean that the Internet service provider is “to **remove** that infringing material as soon as practicable thereafter”; or that otherwise they become “**liable** for the infringement” mean? It did not mandate a court order in these circumstances.²⁴ It is clear that the Copyright and Related Rights Act 2000 was not concerned with Internet theft. Further, no rule of statutory interpretation entitles a judge to turn national legislation into something it is not just because the State has an obligation under European law that is not fulfilled. The European Court case of *Marleasing SA v. La Comercial Internacional de Alimentacion SA* (C-106/89), requires the courts of Member States to construe legislation in accordance with our EU obligations. The European Court made it clear in *Wilhelm Roith v. Deutsches Rotes Kreuz* (C-397/01)²⁵ that this interpretation cannot be so extreme as to do violence to the national legislation, turning it into something that it is not: or as the Court say in a wonderful new Latin phrase, *contra legem*. The relevant European directives were passed over a period of three years and I now refer to a brief chronology.

At the time of the passing of the Copyright and Related Rights Act 2000, the E-Commerce Directive²⁶ 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 Irish 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 2002. This was followed by the European Community (Directive 2000/31 EC) Regulations 2003 (S.I. No. 68 of 2003).

24 [1990] 4 E.C.R. I-4135.

25 [2004] E.C.R. I-8835.

26 European Parliament and Council Directive 2000/31/EC of the 8th June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) O.J. L 178/1, 17.7.2000.

It is not so much important to the result of the *EMI v. UPC* case that a defence was provided in the directives, and relied on by UPC, that they were a mere conduit, not initiating the transmission or selecting the receiver or modifying the information, instead, it was a failure in wording in the Irish copyright legislation that proved crucial. That defence of mere conduit is important since those who are mere conduits of information are exempt from liability. Article 14 of the E-Commerce Directive provides, at subpara. 3, that the defences are not to prevent a court, in accordance with the Member State's legal systems, note please, of requiring "the service provider to **terminate** or **prevent** an infringement". A similar wording is contained in other directives. These are set out in the judgment. The wording used in the European directives refers to interruption, diversion and blocking. In particular, Recital 56 of the E-Commerce Directive provides that: "[u]pon obtaining **actual knowledge** or **awareness** of illegal activities [the service provider] has to act expeditiously to **remove** or to **disable** access to information..." It is best to quote the relevant portions of the E-Commerce Directive in full where we find reference to the possibility of an injunction in specific terms in Recital 45:-

*The limitations of the liability of intermediary service providers [as a mere conduit] 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.*

Article 12 sets out the mere conduit defence to liability and the exception that an injunction may be granted nonetheless:

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.***

This is manifestly not the same as **removing infringing material**; the wording available to the Irish High Court under section 40(4) of the Copyright and Related Rights Act 2000. So here are the European legislation words: **remove, disable, terminate, prevent**. When you use different words in legislation, you clearly mean something different in respect of the use of each word. Something can be taken down from a site, if the site is hosting it. What is hosting? Hosting is where you have a website and that can be anything from your own personal photographs to a commercial organisation that advertises its products to the world at large. These sites are hosted by an Internet service provider which provides space on its large computers; often for free if it is a personal website and for a charge if it is a commercial one. Some sites are so large that no one is hosting their material. PirateBay, the *fons et origo* of the entire problem, is probably one such. In the first action, *EMI v. Eircom*, the case having settled on the basis that an injunction to disable access to the PirateBay website would not be opposed, I granted an injunction against Eircom requiring them to block access to their customers to PirateBay. This was not, as I realised when the later *EMI v. UPC* case was fully argued, the **removal** of material; rather it was a **disabling of access**: PirateBay is always there, people are going on it from time-to-time and by court order would be stopped from doing that. As with the other reliefs sought in the *EMI v. UPC* action, the last case and the one where I had the chance to hear both sides and a lot of expert evidence, the inadequacy of the legislation prevented any appropriate action. CopySense will act so as to detect a transmission and allow a warning. That is not to **remove material**. You may argue that it is to **remove** it when at the end of the 'three strikes and you are out' process you no longer can provide illegal copyright material or get it; this is because then a customer is taken off the service of a particular Internet service provider. More properly, that is **disabling access** to the customer. Global File Registry will interrupt a transmission and then send it somewhere else. That is not the same process; it involves an action that **terminates** the infringement. That may be most properly regarded as **diversion**, but in the process the Internet piracy that the customer seeks is **disabled** in favour of a lawful alternative. Detecting a transmission, sending letters, and then ultimately cutting a person off from Internet service, is certainly ensuring that transmissions in breach of copyright cannot occur again, and that is what the music industry argued in court, but that is not the **removal** of the relevant material. Any such court order would operate in order to **prevent** the infringement. Irish legislation does not go as

far as it should under the European directives that I have quoted. I understand that revision is being urgently looked at. In Britain there is compliance with the requirement to implement European legislation effectively and fully, though just how that compliance should work out is still being considered by OfCom.²⁷ Finally, I note that even prior to the Digital Economy Act 2010, the statutory instrument implementing the European directives in the United Kingdom used the four words I have quoted above, only one of which appeared in the Irish legislation.²⁸

Data Protection

In a separate judgment entitled *EMI v. Eircom*²⁹ I analysed the three strikes solution as best I could. The Data Protection Commissioner asked three questions of the Court but did not appear in the hearing because of a risk that costs might be awarded against him. These are the three questions:

1. Do data comprising IP addresses, in the hands of EMI or its agent(s), and taking account of the purpose for which they are collected and their intended provision to Eircom, constitute “personal data” for the purposes of the Data Protection Acts, 1988-2003, thereby requiring that the collection of such IP addresses by EMI or its agents must comply with the specific requirements of each of section 2, 2A, 2B, 2C and 2D of the Data Protection Act, 1988 as amended?
2. Having regard to section 2A(1) of the Data Protection Act 1988 as amended, and assuming for current purposes that the processing by Eircom of “personal data” in the context of the third of three steps envisaged by the graduated response scheme proposed under the terms of this settlement, (i.e. the termination of an internet user’s subscription) is “necessary for the purposes of the legitimate interests pursued by [Eircom]”, does much processing represent “unwarranted [processing] by reasons of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject”?
3. Having regard to section 2A(1) and 2B(1) of the Data Protection Act 1988 as amended, is it open to EMI and/or Eircom to implement the graduated response process set out in the terms of the settlement including, in

²⁷ See also, in this regard, *R (British Telecom) v Secretary of State for Business, Innovation and Skills* [2011] EWHC 1021 (Admin) where the Court rejected a number of objections made to the Digital Economy Act 2010, including the argument that the Act was disproportionate.

²⁸ See The Electronic Commerce (EC Directive) Regulations 2002, No. 2013 of 2002 of the UK.

²⁹ *EMI Records v. Eircom plc.* [2010] IEHC 108 (High Court, Unreported, Charleton J., 16 April, 2010)

particular, the termination of an internet user's subscription under step 3 of that process, in circumstances where:-

- (a) In doing so they would be engaged in the processing of personal data and/or sensitive personal data (in so far as the data can be considered to relate to the commission of a criminal offence), including the provision of such data from one private entity to another private entity; and

The termination of an internet user's subscription by Eircom would be predicated on the internet user in question having committed an offence (i.e. the uploading of copyright-protected material to a third party by means of a peer-to-peer application) but without any such offence having been the subject of investigation by an authorised body; and, further, without any determination having been made by a court of competent jurisdiction, following the conduct of a fair and impartial hearing, to the effect that an offence had in fact been committed.

Because privacy was maintained, because there was no central register of those cut-off set up, and no sharing of information among Internet service providers of errant customers, and because the information was not to be used publicly for criminal prosecutions, or even tort actions, the Court held that there were no data protection infringements. Our law in Ireland is based on the European Directive. I have been passionately criticised and it has been said that the judgment does not have enough, or any, regard for data protection and for privacy rights. A judge is open to criticism. I am not entitled to defend any decision of mine by adding to it or subtracting from it. The European Data Protection Supervisor (EDPS) had a different view. He regarded the gathering of IP addresses as a breach of privacy. He thought that there was disproportion to a three strikes solution and that education ought to be pursued as a proportionate response.³⁰ In the evidence before Court in the *Eircom* cases, the music companies had stated unchallenged that after obtaining *Norwich Pharmacal* orders that they had done all in their power to publicise that copyright theft might be detected. This had led to a drop in piracy, but only for a matter of a week or two before figures for illegal downloading climbed up and beyond where they had been before. The EDPS was also of the view that what was involved was the processing of sensitive information related to criminal offences. The Court in the *Eircom* case took the view that vast swathes of law were concurrent torts, or civil wrongs, and crimes, an example being that in Irish law every breach of tax law is a civil offence and a crime, but that since the music companies had no interest in

³⁰ Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA), O.J. C-147/01, 5.6.2010. Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:147:0001:0013:EN:PDF>,

either identifying or prosecuting the offenders that the definition of sensitive information was not applicable. What they were interested in was a private, between the internet service provider and the customer, system of warning and discontinuance of Internet service not criminal prosecution. Finally, I thought that Eircom had a legitimate interest in upholding the rule of law, in avoiding threatened litigation and in enforcing their contracts with customers which provided for discontinuance in the event that the customer used Internet service to steal copyright. It should be noted that there are always two possible views on any issue.

Judicial Discretion and Judicial Activism

Since the Internet service providers are not actually stealing anyone's copyright, but are a means to do so, European law provides for both a mere conduit defence in an action for damages and also for injunctive relief despite that defence. That does not mean that an injunction is automatic once it is properly provided for by transposition of the directives. Injunctions invoke the discretionary jurisdiction of the courts and, in the famous words of Lord Blackburn in *Doherty v. Allman*,³¹ that jurisdiction is "not one to be exercised according to the fancy of whoever is to exercise the jurisdiction of equity".³² In *American Cyanamid Co. v. Ethicon Limited* Lord Diplock set out the test for the granting of interlocutory injunctions on the basis that "[t]he court no doubt must be satisfied that the claim is not frivolous or vexatious, in other words, that there is a serious question to be tried."³³ This test was embraced by the Irish Supreme Court in *Campus Oil Limited v. Minister for Industry and Energy (No. 2)*.³⁴ It may seem simple but it poses a dilemma to every judge who is requested to grant injunctive relief on an interlocutory basis: is this order absolutely necessary in the light of its attendant consequences and should I make it on the basis of such a slight test? The significance of the consequences is what is immediately in any judicial mind should an injunctive order turn out to be wrong decision. After all, it is not an order based on a finding of fact, only an order based on a "serious issue". In a recent English High Court decision, Clarke J. put one possible judicial response to a motion for injunctive relief this way: "a fundamental principle is that the court should take whatever course appears to carry the lower risk of injustice if it should turn out to have been the "wrong" course"³⁵.

That risk must weigh heavily on the deliberations of any judge even when there has been a full hearing. The injunctive jurisdiction is, of its nature, one of balance and

31 (1978) 3 App. Cas. 709.

32 Ibid, at p. 728.

33 [1975] A.C. 396, at p. 407.

34 [1983] I.R. 88.

35 *SabMiller Africa B.V. v. East African Breweries Limited* [2009] EWHC. 2140 (Comm), para. 48.

has been so since the Supreme Court of Judicature Act 1875 allowed the civil courts to issue an injunction where it is shown to be “just and convenient”.

The grant of a final injunction should always call to mind its consequences. To fail to abide by it is a civil contempt. The remedy is imprisonment, or in the case of a corporation, sequestration of property. A judge has to be sure, therefore, that making an order injuncting some activity or process is right. Furthermore, those that come under the sway of an injunction must know what is permitted and what is forbidden. It must also be possible for those individuals to comply with it. As Kekewich J. in *Evans v. Manchester, Sheffield and Lincolnshire Railway Co.* put it as far back as 1887:

*I think it would be wrong to enjoin a company or an individual from permitting that to be done which is really beyond his control... in the sense that he cannot by any precaution or any works with reasonable certainty comply with the order that is sought.*³⁶

Equity has developed a number of maxims or guiding rules to assist the courts in issuing injunctions. A non-exhaustive list includes that the remedy must not be futile, it must not impose an obligation impossible to abide by and nor should it be granted where damages would be an adequate alternative. In *Attorney General v. Colney Hatch Lunatic Asylum*³⁷ Hatherley L.C. observed that the courts must “take care not to pronounce an idle and ineffectual order”. An Irish repetition of this principle can be found in *Meath Co. Council v. Irish Shell Ltd.*³⁸ where Lavan J. endorsed the well rehearsed dictum of *Brewster L.C.* in *Sheppard v. Murphy*³⁹ to the effect that “a Court of Equity cannot compel [anyone] to do that which is impossible”.

These concepts only touch upon the principles and factors that a court might consider when determining whether or not an injunction is appropriate. Others, according to Kirwan, include:

- (a) whether alternative remedies are available;
- (b) the effect of granting an injunction on third parties;
- (c) damage, hardship and oppression;
- (d) collateral benefit;
- (e) the separation of powers;
- (f) the *bona fides* of an applicant;
- (g) illegality;

³⁶(1887) 36 Ch. D. 626 at 639.

³⁷ (1888) L.R. 4 Ch. App. 146.

³⁸ Unreported, High Court, Lavan J., 12th June, 2006.

³⁹ [1868] I.R. 2 Eq 544.

- (h) frivolous and vexatious applications; and
- (i) status of an undertaking.⁴⁰

There is an acute awareness that justice, unrestricted by principle and reality, has the potential to do greater harm than good. Although made in the context of estoppel, the comments of Weeks J. in *Taylor v. Dickens* must be borne in mind for every judge exercising his or her equitable jurisdiction:

*In my judgment there is no equitable jurisdiction to hold a person to a promise simply because the court thinks it unfair, unconscionable or morally objectionable for him to go back on it. If there were such a jurisdiction, one might as well forget the law of contract and issue every civil judge with a portable palm tree. The days of justice varying with the size of the Lord Chancellor's foot would have returned.*⁴¹

In the context of Internet piracy injunction applications, there may be considerations about requiring not fully-tested machinery to be engaged in diverting or interrupting what might otherwise be lawful communications. What if the software does not work? What if the order is uncertain in its terms; one that requires a defendant to make reasonable efforts to effect a solution or to employ a reasonable number of people on the customer interface programme? That issue exercised the mind of the Advocate General in *Scarlet Extended*. One of the principles in European law is “prevue par la loi”.⁴² A person is entitled to know what the law is; what it demands; how judges are empowered; and what he is likely to be facing in the event of a breach. How does that square with a judge being asked to grant an injunction on the basis of an untried technical solution? What about the rights of third parties whose transmissions may pass through an internet service provider's network? How much resources are each side to put into a technical or into a graduated response solution? This series of problems is possibly one of the reasons why it is appropriate that the legislation in Britain engages with the task of testing out potential solutions before any injunctive relief is granted. OfCom, the British telecommunications regulator, tests software and can make regulations as to its use. The effectiveness of any response to Internet piracy can then be seen by reports that are put in front of the judge as to which machinery can be expected to work and how much in terms of resources it may need. In some litigation disputes this can be predicted to be essential information.⁴³

40 See Kirwan, 'Injunctions, Law and Practice' (Thomson Roundhall, 2008), in particular, chapter 4.

41 [1998] F.L.R. 806.

42 See paragraphs 92 to 96 of the opinion of AG Cruz Villalón in Case C-70/10 *Scarlet Extended v Société belge des auteurs compositeurs et éditeurs (Sabam)*.

43 In April of last year, the U.K. Digital Economy Act 2010, came into force. This legislation followed a period of intense consultation and debate between ISPs and copyright owners. For a long time the British Government seemed content to support an industry led solution to this difficult issue. However, under the Act, if a voluntary code fails to materialise then Ofcom (the Communications Regulator) will be obliged to introduce its own mandatory code.

And then there is the vexed question of judicial activism, part of the penumbra, but at the opposite end, of judicial discretion in the grant of injunctions. On our side of the Atlantic, the European Council and Parliament have set out the law on copyright in exhaustive detail. Copyright is established on a supra-national basis. The remedy is damages. Injunctive relief is available against mere conduits, provided there is a legislative basis to disable, remove, terminate or divert Internet communications and an injunction is appropriate. There is no mention of the imposition of third party liability on the basis that the machinery of a defendant is used for infringement; or in other words a return to the indecisive ‘authorisation of breach of copyright’ jurisdiction. Where, after all, would any such judicial activism of that variety leave the mere conduit defence established by European law? It may be that the decision of the United States Supreme Court in *MGM Inc v. Grokster Ltd*⁴⁴ might be argued in that regard. But to so respond at least some degree of activism is required and the field is already replete with legislation. That might be predicted by some to make such a development improbable. It can be argued as well that the reasoning behind *Grokster* is to move criminal law concepts of deliberation and even of incitement into the civil area, in the sense that the United States Supreme Court established liability on this basis:

We hold that one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps

On 28th May, 2010 Ofcom, issued a draft initial obligations code⁴³ (“the draft code”) for ISPs under the Act. Under s. 3, which inserts s. 124A into the Communications Act 2003, ISPs are required to notify subscribers alleged to have infringed copyright, as well as to provide copyright owners with lists (on an anonymous basis) of serious repeat infringers. It is hoped that these notices will act as a significant deterrent and that no further steps will be required. However, under ss. 9 and 10 if such measures have failed, the Secretary of State can require Ofcom to take steps to ensure that “technical obligations” can be imposed on ISPs. “Technical obligations” are defined as measures that:-

- (i) limits the speed or other capacity of the service provided to a subscriber;
- (ii) prevents a subscriber from using the service to gain access to particular material, or limits such use;
- (iii) suspends the service provided to a subscriber; or
- (iv) limits the service provided to a subscriber in another way.

Under the draft code there will be a three step notification procedure. Step involves the issuing of a copyright infringement report (“CIR”) to an ISP which will followed a format agreed between the rights-holders and ISPs. Importantly, these reports must set out the method used to gather the evidence of infringing activity. Step 2, the notification step, is triggered on the receipt by the ISP of the CIR. The first CIR will set out the obligations and potential consequences for any infringers. If a second report is received on or after a month of the first report, then a second notification letter will be issued. If at this point the subscriber has failed to heed the warnings and infringes for a third time, then one of the technical measures set out above may be invoked.

There is also an appeal to a special tribunal to be established by Ofcom. Thus, the code leaves no uncertainty at any point as to the obligations and responsibilities of all the key players involved: namely, copyright owners, ISPs and internet subscribers. This clarity and certainty is to be contrasted with the Sabam Opinion set out above, and also the uncertainty surrounding the technical solutions urged on the Court in *E.M.I. v. UPC*.

44 (2005) 545 US 913. On this line of cases, see also *Religious Technology Centre v Netcom On-Line Communications Services Inc* (Cal 1995) 907 F Supp 1361; *A and M Records Inc v Mapster Inc* (9th Circuit 2001) and *Sony Corporation v Universal City Studios* (1984) 464 US 417.

taken to foster infringement, is liable for the resulting acts of infringement by third parties.

One might be forgiven for wondering, especially as the judgment against Groakster resulted in damages of \$50 million and the liquidation of the corporation, if European judges would step aside from a clear legal framework to develop copyright law in this way?

Concluding Thoughts

In Ireland in 2010 it was not possible to grant an injunction to outlaw Internet piracy: neither in respect of three strikes and you are out or to disable access to the PirateBay. The law may soon be changed under our new government. It is certain, however, that the technical solutions outlined before the High Court, and the debate about the necessity for intervention, the relevance of privacy and the entitlement to access to judicial scrutiny will continue. As Professor Phillips told the Fordham Intellectual Property Conference in April 2011, the decisions of the European Court of Human Rights and of the European Court have tended to value rights as to privacy, information and copyright, but in that order of importance.

Some may argue that a clear line is needed. Either we have copyright protection or we do not. Britain has the advantage of carefully thought-through legislation. Indeed, in the recent decision of their High Court in *R. (British Telecom) v. Secretary of State for Business, Innovation and Skills*⁴⁵ challenges brought by the U.K.'s leading Internet service providers to the provisions of the Digital Economy Act 2010 were rejected. Parker J. was satisfied that the system introduced under the Act and by Ofcom represented an efficient, focussed and fair system. Moreover, the Court was impressed by the transparency and decisiveness of the legislation, noting that it provided clarity for all involved in the process. Legislation such as the Act of 2010, has at least the predictability of express statement as to the objects to be achieved. In respect of each of the possible solutions of diversion, interruption, warning and cut-off, the British have OfCom looking at the appropriate technical machinery with which to achieve these ends. When this machinery is approved, then, in those circumstances, any court faced with these difficult cases will be in a position to fairly, if not precisely, predict what they can use as a technical solution with a view to granting or refusing to grant injunctions. This strongly accords with the European law principle that the law should be predictable as to what is mandated and what is forbidden and enables a judge to also know what is expected in the judicial sphere in particular circumstances. As I said in another part of the judgment in *EMI v. UPC*, if any judge were merely to act on the basis of what the Court felt was right,

⁴⁵ [2011] EWHC 1021 (Admin)

without having a legislative basis, the Court would be putting itself back in the position of judges in the late 19th and 20th century who used the tort of conspiracy and the remedy of an injunction against the trade union movement and thereby caused public controversy, rendered uncertain the concept of the rule of law and undermined their own authority.

It may also be well for the judicial mind to observe that the separation of powers is a definite guiding principle against doing what might seem desirable, but which is not provided for in legislation.