Neutral Citation Number: [2010] IEHC 108

THE HIGH COURT

2008 1601 P

BETWEEN

EMI RECORDS (IRELAND) LIMITED

SONY B.G. MUSIC ENTERTAINMENT (IRELAND) LIMITED,

UNIVERSAL MUSIC IRELAND LIMITED, AND

WARNER MUSIC IRELAND LIMITED

PLAINTIFFS

AND

EIRCOM LIMITED

DEFENDANT

JUDGMENT of Mr. Justice Charleton delivered on 16th April, 2010

1. A settlement has been effected in the litigation between the parties. Its purpose is to diminish the theft of copyright material over the internet. The infringers are to have their service cut off. This judgment concerns the compatibility of what the parties have agreed in relation to data protection legislation. The substance of the original case concerned the stealing of copyright-protected sound and video recordings over the internet, mainly by peer-to-peer sharing groups. Eircom Limited, the defendant, is an internet service provider and some of their customers, among others, engage is this activity. Nothing suggests any willing infringement of copyright by Eircom, or that they were in any way a party to copyright theft. That, however, does not mean that an injunction cannot justly and conveniently be granted against a conduit for copyright infringement; a point to which I will return. The plaintiffs are big players in the music and film industry. They represent sound recording and motion picture artists who have assigned their copyright in new original creative work to them in exchange for financial backing, promotion and the protection of a commercial organisation to further their interests. Remuneration for that kind of work is shrinking by reason of copyright theft over the internet. I will describe the process shortly.

2. Since the parties in this case resolved their differences, after eight days of evidence, it was not necessary for the Court to make an order. On 28th January, 2009, terms of settlement were set down in writing and filed in court. The implementation of that settlement raises issues under the Data Protection Acts 1988 and 2003 and, in consequence, the terms agreed must be scrutinised by the Court to analyse its compliance with that legislation. Because a large amount of computerised data was involved, one of the parties communicated with the Data Protection Commissioner to seek his advice. He, in turn, raised three issues as to why the settlement might be doubted to conform with the legislation as to the manner of its implementation. By order of Kelly J. made in the Commercial Court motion list, and dated 18th January 2010, I am asked to rule on these issues. Hence, this judgment is given after argument by the parties to the main case. The Data Protection Commissioner did not appear because of a concern over indemnity as to his costs. I will shortly recite each issue and my conclusion thereon but, firstly, I need to refer to some background.

Background

3. The problem faced by the plaintiffs is extremely serious. Many talented artists have assigned copyright in their musical and cinematic work to them. In common with many other occupations, those working in the music and film industry may be at the very top of the earnings ladder or at the bottom without even a foot on the first rung. Most will be somewhere in between. It is of no interest to me as to whether people hold views that the music and film industry either over-rewards or unfairly-exploits its artists. Copyright is a universal entitlement to be identified with and to sell, and therefore to enjoy, the fruits of creative work. It applies to everyone who manages to produce anything copyrightable from a song, to a telephone directory, to a symphony, to a film. Were copyright not to exist, then the efforts of an artist could be both stolen and passed off as the talent of another. Were the artist not entitled to exploit her or his creation by preventing others from copying it without permission, usually for a fee, then the fruits of moments of inspiration worked out through weeks of endeavour and representing, sometimes, the distillation of some fundamental experience of life, would bring no reward, perhaps not even applause. Even if an artist won acclaim, it alone would not keep body and soul together. Examples of what can occur where copyright protection is absent used to be found as notorious examples of unfairness in history rather than as a contemporary situation that has developed because of the abuse of the internet. When Jan Sibelius, a Finn, penned his Valse Triste, Finland was part of the Russian Empire, not a party to the copyright convention, and the great composer received nothing for what was then his most popular work. The three early ballets of Igor Stravinsky, a Russian, suffered the same fate; though on moving to the West, the composer re-orchestrated them and republished them gaining copyright but only in that form. No reasonable person doubts the injustice of that situation. The law does not doubt it either.

4. When the internet gained wide currency in the 1990s many of its adages began to believe that a new form of reality had been created. Some felt that it should be subject to no rules since, as it was not based in a particular country, but as its name implies is a world-wide web of communication, unlike the previous means of communication through the post, by telephone, through television or through films, it seemed to be impossible to subject to local regulation. That is not so. Nor should it be. In common with other aspects of life, the internet has both a positive and a dark side. On the positive

side, its aids free communication; it opens up avenues of knowledge so that it has become a centre of learning in itself; it furthers public debate; and has established the swiftest and most far reaching form of communication that humanity has known. It is, on the other hand, also thickly populated by fraudsters, pornographers of the worst kind and cranks.

5. The internet is only a means of communication. It has not rewritten the legal rules of each nation through which it passes. It is not an amorphous extraterrestrial body with an entitlement to norms that run counter to the fundamental principles of human rights. Since the early days of the internet, and increasingly as time has gone on, copyright material has been placed on the World Wide Web by those with no entitlement to share it. There, it is downloaded by those who would normally have expected to pay for it. Among younger people, so much has the habit grown of downloading copyright material from the internet that a claim of entitlement seems to have arisen to have what is not theirs for free.

6. How is this done? The internet consists of millions of connected computers with linkages established by many thousands of internet service providers operating very large computers. The defendant Eircom is one of these. Normally, an internet service provider could not be expected to control the contents of what flows over the communications channel between its customers, who pay them for internet service, and others on its network, or elsewhere on the World Wide Web. Before this case, Eircom did not monitor its customers. It provides a service and lets the customer proceed with enjoying the benefits of that. This freedom does not exempt the customer from criminal or civil liability. There is nothing in the criminal or civil law which legalises that which is otherwise illegal simply because the transaction takes place over the internet. Child pornography, for instance, remains child pornography whether sent by post or digitally transmitted.

7. Those who wish to obtain, or to share, copyright material which belongs to others, without acknowledgement of their rights and without payment, frequently join a peer-to-peer network. This may consist of a swarm of thousands of computers which are all on line at any one time and connected through internet service providers. To obtain the relevant software for downloading complex material in musical or cinematographic form, an internet user can go to an illegal site. Legal downloading of free material is also becoming increasingly popular on sites hosted by, for instance, national radio and television broadcasters. Many television and radio networks store material for legally downloading for free from their television or radio archives, or for listening or seeing again, using an 'i-Player' system, or something similar. This can be accessed on their websites, and links to the relevant software as a free service are often provided. The software for peer-to-peer illegal downloading, on the other hand, is obtained from such sites as Pirate Bay. That is only an example. As I understand the evidence that I heard, internet sites like that one supply two basic things. Firstly, they will allow downloading of the relevant software for peer-to-peer illegal file participation. Secondly, those so inclined can learn from such sites what swarms of active computers contain the material that they want to filch. Then, a person so inclined will open up a new file on their computer with the relevant newly-downloaded software. This enables a peer-to-peer download. It also makes each downloading participant an uploading participant whereby others in an active swarm will load from each other participant. This happens because of the peer-to-peer software and it happens whether a participant wants it to happen or not. Whatever is within the peer-to-peer file that is necessary for illegal downloading on a computer will be copied as a participant downloads and will be sent over the internet, through the internet service provider, and into, and from, the participant's computer. This is a complex activity and used to be very slow. Using high speed broadband quickens the process. That which used to take hours can sometimes now be completed in minutes. As to a song or a video, it does not all come from, nor is it all taken from, the same participant. Again, reviewing the evidence that I heard in this case, it seems to operate like this: each digital encoding of a musical or cinematographic work is split up into miniature files. These may last a couple of seconds in real time when played. They, as well as being in digital language, have a beginning and an end code in digital format. Since internet technology is partly about the shortest route of communication, the peer-to-peer software enables the illegal downloader to obtain a few seconds here, there and elsewhere from participating swarms. The overall file of the work will be identifiable in the beginning and end codes and within the intermediate codes. These will arrive randomly, a bit like a computer image building up on the screen, and be put together by the computer software docking the beginning and end codes of each of the few seconds into a complete and chronologically correct entity. While a participant is downloading this material, each participant's own computer engages with the swarm so that every music song or video in the relevant file of each individual computer becomes available to thousands of other users around the world. They will mutually download, and so illegally share material, in the same way.

8. In general, no one will come knocking on the door of any of these people. Up to the terms of settlement agreed between the parties in this case, moreover, no internet service provider had apparently agreed to attempt to tackle this copyright-repugnant situation of their own volition. From the point of view of the participants, everyone seemed to win; except for the creators of original copyright material who were, and are, utterly disregarded. It is only common sense that this attraction of free, but illegal, downloading of the latest songs and videos made the sale of internet access attractive. Those who wished to filch the copyright material of others had to provide others with material to be filched from them. The more the participants, it seems, the easier the internet route. The only downside to participation, mentioned in the course of the hearing, is that the mischievous side of the human personality, containing a repulsive aspect as well as an attractive and humorous one, has also come to the fore over the internet. Using these networks exposes participants in the swarms to severe computer-crippling viruses.

The Settlement

9. Because this process takes place over the internet in generally unencoded form, software has been developed to detect illegal downloaders. One such was referred to in evidence as DtecNet. This is one of the current technology market leaders, but if encoding of illegal sharing of copyright material increases - it is now in its infancy - technology for detection will have to forge ahead also. Companies operating this or similar services are hired by the plaintiffs. Under the terms of the settlement, these companies tell the plaintiffs that a particular computer has been involved in illegal file sharing of its copyright material. This information is passed by one of the plaintiffs to the defendant Eircom, as the internet service provider. It then informs its subscribers that they have been detected infringing copyright. If there is a second occasion of illegal downloading, Eircom is obliged, when so informed, under the settlement to write to the subscriber warning them that unless that sort of infringement ceases, they will be disconnected from general internet service. This disconnection does not apply to any telephone or television service that a subscriber gets over their internet facility. On a third infringement, that discontinuance is implemented by Eircom: the subscriber is taken off service except for phone or television internet access. This is a serious sanction. Some would argue that it is an imposition on human freedom. There is no freedom, however, to break the law. Further, while it is convenient to have internet access at home, most people in Ireland have only to walk down to their local town centre to gain access for around €1.50 an hour. The

parties also agreed, under the settlement, to negotiate a protocol setting out the details of the precise procedure for implementing this settlement.

10. Since it was likely to be deeply unfair that only Eircom with about 40% of the market share, as the defendant in these proceedings, should bear the burden of this settlement, thus activating the winds of market forces to drive customers towards Eircom's competitors, the plaintiffs agreed to initiate similar proceedings against other internet service providers in the State. This, I understand, has been done. That case is in the Commercial Court list for hearing on 10th June, 2010. In addition, Eircom agreed not to oppose an application by the plaintiffs to injunct the Pirate Bay site. I have already given judgment on this *ex tempore*, closing down access to that site through Eircom; see *EMI v. Eircom,* [2009] IEHC 411, (Unreported, High Court, Charleton J., 24 July, 2010).

The Protocol

11. The settlement was always going to be difficult to implement precisely. The parties agreed, as part of it, to negotiate a protocol governing their respective sides of the bargain. I wish to refer to the main points. There has to be an education and awareness campaign by Eircom, directed at its internet customers, about the abuse of peer-to-peer software, securing broadband installation in the home and how signs of copyright infringement might be detected by the main householder. A lot of this seems predicated as likely to happen at teenager or slightly older level. The implementation of the settlement was to be phased in by a three month pilot programme; because this was the only way the parties could see how things were working and to analyse how practical their measures might be proved to be. There were to be exceptions to the ultimate sanction. Some people might be depending on their broadband internet access for medical services and others for their livelihood. Where an infringement took place within a business, but contrary to the internet use policy within the organisation, communication by way of admonition might replace the ultimate measure of shutdown. Other categories of exception might grow over time. In terms of privacy, there are two provisions which are relevant to the data protection legislation to which I shall shortly turn. Under para. 2.10 of the protocol, where an exception to shut down after a third infringement occurs in the manner provided for, Eircom will only communicate with the relevant plaintiff to the effect that "this IP address does not fall with the terms of the protocol". Under para. 2.3, notification by one of the plaintiffs to the defendant that there has been an illegal downloading of their copyright material consists of details of the copyright holder (which could be, for example, a particular songwriter); that a breach of copyright has occurred; details of the relevant album or song or video; the IP address that has been detected in infringing copyright; and other details that show proper investigation, namely, the relevant software used and the digital fingerprint of the copyright material used.

12. Then one moves on to the three infringement levels under the protocol. Nothing in these provisions changes one basic fact. Neither DtecNet, or any similar service of detection, nor any of the plaintiffs whose copyright material is being infringed would ever know through this process that the infringer is a particular person living in a particular place in Ireland. What they do know is that a particular IP address has been involved in the downloading. An IP address is the number given to a computer from an internet service provider when it receives internet access. The IP number electronically identifies the user of the internet. Banks of numbers for IP addresses are produced by an international organisation and these, in turn, are provided to internet service providers. One can find out by looking at the IP number, I understand, who the internet service provider is. What internet service provider is given what bank of thousands or millions of IP numbers is not kept a secret anywhere. Since each internet service provider will have, in turn, many thousands of customers, one is not moving much closer to finding out the identity of an internet abuser by knowing the copyright infringing IP address was assigned to that company. That number will probably give you no more than an indication of the domicile of the computer. Further, I am convinced, on the basis of the affidavit evidence before me, that the plaintiffs have no interest at all in using this process to find out who the copyright infringers are. Rather, what they are interested in is having the protocol work so that the plague of copyright infringement may be undermined.

13. On the first infringement, the bill payer at the IP address will be told with their bill that an infringement was detected at such and such a time in respect of a particular song, or whatever it is, that is subject to copyright. This enables them to reflect on their conduct or to communicate with the rest of their household. On a second infringement, a formal letter is received by the customer from Eircom. This is to the same effect, but it will presumably be couched in stronger terms than the warning with the bill. The customer can only go to level 2 after fourteen days have passed since the first infringement. As I understand it, these communications may also contain information concerning how to keep one's computer secure from, for instance, the person next door and other continuing education tips. When a third infringement notification is received by Eircom from one of the plaintiffs, after a further fourteen days, Eircom must then review all the evidence. This is done on a human basis; the first two levels operating automatically. A termination notice is then issued to the customer giving fourteen days before cut-off. The customer is then entitled to make representations to Eircom, as the internet service provider, over the telephone or through the internet. The user's representation is considered by Eircom, not in consultation with the plaintiffs, under para. 2.8 of the protocol. Private matters involving extenuating circumstances, so as to call into play one of the exceptions, or material whereby it is claimed as a matter of fact that the infringement has not taken place at all, must be considered by Eircom. Then, if that does not cause the consequences of the protocol to be diverted or postponed, the customer is cut-off from internet service.

The Eircom Subscriber Contract

14. Eircom provides internet service to its customers based on a written contract. This document is very strong in the pact which a customer makes with Eircom not to use the internet for illegal purposes. Under clause 2.1 of the agreement, the customer agrees to avail of the facility of internet service subject to the terms and conditions set out in the written document. Among the matters which the customer has to agree to is not to use the facility to create, to host, or to transmit obscene or racist material; clause 5.3. The customer must agree not to use the facility of internet access to infringe the propriety rights of any software; clause 5.6. Under clause 5.10, the customer agrees that the internet service can only be used in accordance with the acceptable usage policy posted in clear terms on www.eircom.net. This site displays a clause very similar to clause 5.5 of the contract which, because of its importance to the issues which follow, I should now quote:-

> "Customers may not use the facility to create, host or transmit material which infringes the intellectual property rights including, but not limited to, the copyright of another person or organisation".

15. Clause 7.1 provides that the agreement may be suspended or terminated by Eircom for breach of its terms. It is important to recall that it is one of the basic functions of the courts under the Constitution to give effect to lawful agreements.

The Issues Raised

16. By letter dated 4th December, 2009, the Data Protection Commissioner wrote to the solicitor for the plaintiffs raising a number of concerns as to the lawfulness of the settlement terms. These were later, on the 15th January, 2010, encapsulated by Philip Lee, solicitor, in a precise form for which the Court is grateful. These are the three issues:-

> "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 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
> >
> > (b) 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."

17. I now propose to address each of these issues in turn and to rule on same.

Issue 1

18. Here, for the sake of clarity, is issue 1 again:

> "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?"

19. Personal data is defined by s. 1 of the Data Protection Act 1988, as amended by the Data Protection (Amendment) Act 2003, as:-

> "Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller."

20. Under the same section of the Act, the data controller is defined as meaning a person who, either alone or with others, controls the contents and use of personal data. What is involved in the first, second and third step of the protocol is the scanning by either the plaintiff personally, or more likely through computer agencies hired in that regard, of the entire internet network to see whether any infringement of copyright material is taking place. Attention is likely to be focused in Ireland for these purposes. Using software such as DtecNet, their efforts will gain two basic pieces of information. Personalising DtecNet, for the moment, it, as a computer programme is only interested in the copyright material of the plaintiffs, or one or other of them. Continually scanning and rescanning internet communications, it finds the material being transmitted in various directions from peer-to-peer, or similar, swarms and, in effect, follows the communication down the line until it ends up in a particular computer and takes note of its IP number. In the course of the case, I heard that some computer firms are also developing automatic systems to cut copyright infringing communications prior to completion; but that is not relevant here. In some way, perhaps because the signal runs two ways, at least after the first illegal download, DtecNet and similar systems are able to find out the IP address and what infringement of copyright material has taken place. This is the material that is then collected in blocks and delivered to one or other of the plaintiffs. As I have previously indicated by reference to the protocol, none of this material gives any clue as to the name of the main householder, or business, or café in which the computer is situated or whether it is in An Gorta Choirce in County Donegal or in Ranelagh in Dublin.

21. I need to refer here to what processing means under the Act, as amended. This is set out thus in s. 1, the definition

section:-

> "Processing, of or in relation to information or data, means performing any operation or set of operations on the information or data, whether or not by automatic means, including -
>
> (a) obtaining, recording or keeping the information or data,
>
> (b) collecting, organising, storing, altering or adapting the information or data,
>
> (c) retrieving, consulting or using the information or data,
>
> (d) disclosing the information or data by transmitting, disseminating or otherwise making it available, or
>
> (e) aligning, combining, blocking, erasing or destroying the information or data;"

22. An Act should never be split up into its constituent pieces and then analysed as if each were disconnected from the broader purpose that constitutes the legislation. Insight is often gained as to the meaning of a particular section, or indeed a definition, by showing how it is used in conjunction with other sections, or by analysing how the same concept is dealt with elsewhere. The definition of disclosure in s. 1 of the Act assists in this regard. That definition states:

> "Disclosure, in relation to personal data, includes the disclosure of information extracted from such data and the transfer of such data but does not include a disclosure made directly or indirectly by a data controller or a data processor to an employee or agent of his for the purpose of enabling the employee or agent to carry out his duties; and, where the identification of a data subject depends partly on the data and partly on other information in the possession of the data controller, the data shall not be regarded as disclosed unless the other information is also disclosed".

23. I do not accept fully the dictum of McMullin J. in *Transport Ministry v. Simmonds*, [1973] 1 NZLR 359 at 363 as to what the word "likely" means when used within a statute. To be personal data, under the Act, the information has to identify a living individual from the data or from data in conjunction with other information in the possession of the data controller, or from other information that is likely to come into the possession of the data controller. McMullin J. says that the word likely can be used in many contexts and that its meaning has to depend upon the particular context of the statute or regulation. That is hard to disagree with. He refers to an event which is likely in terms that it "may be an event which is probable but it may also be an event which, while not probable, could well happen". In addressing juries, judges in this jurisdiction refer to the civil standard of proof as being that a fact is shown to be more likely than not; in other words, more probable than not. In referring to a sporting fixture, the pundits will say that one team, rather than another, is the likely winner. Where a group of teams is involved, the most likely winner may be identified and, in that context, the word may be used to mean something other than probable. If likely does not mean probable in a particular context, it at least means something akin to probable. I agree with McMullin J. that the word "likely" has no relevance to any concept such as a bare possibility, and I am rather inclined to believe that in most, if not all, statutory contexts that likely means probable; no more or less than that.

24. The previous approach of the plaintiffs to the problem which I have described was to apply for what are now called *Norwich Pharmacal* orders; named after the House of Lords decision in *Norwich Pharmacal v. Customs and Excise* [1974] A.C. 133. That order involves an application against an innocent party, such as Eircom, to disclose information because a civil wrong is being, or was being, perpetrated against the plaintiff and because the defendant, though not a party to the wrong, can identify the tortfeasor. In *EMI Records v. Eircom Limited* [2005] 4 I.R. 148 Kelly J. made such an order against the defendants in the context of the activity that I have described earlier in this judgment. The plaintiffs were then exploring obtaining information by court order in civil proceedings as to who was infringing copyright over the internet and then following up on that by further legal action. I do not regard it as relevant whether that further action might be criminal or civil. The purpose of this settlement is different. Kelly J. made an order that Eircom should disclose the names of its infringing customers, the plaintiffs having first supplied a tranche of IP addresses together with evidence of copyright infringement. That order was made on the basis that there had been a demonstration of wrongful activity by unknown persons who were internet subscribers of Eircom whereby copyright assigned to the plaintiff was being infringed. The stated purpose of such an order was to enable the plaintiff to then directly take action against each such illegal downloader. Kelly J. considered in depth the issue as to whether the information required could be obtained elsewhere than from the defendant. The action in question is pointless, in terms of the practical application of litigation tools, and the *Norwich Pharmacal* order is not allowable as a matter of law, unless the only practical way of obtaining the identifying details is through the suit. Since the High Court has made such an order in the context of this problem, I regard it as beyond doubt that it was both necessary to make the order disclosing the tortfeasors and that the judgment conformed with the requirements of the procedure that is so clearly set out in the judgment of Kelly J. The difference between that order and this settlement, is that the plaintiffs have left behind what they reasonably regard as an expensive and futile pursuit of the identity of copyright tortfeasors in favour of injunctive relief that has been expressed in the settlement of this case as a protocol to choke off the problem in a three stage process that never involves the identification of any wrongdoer.

25. In consequence, I conclude, that none of the plaintiffs have any interest in personally identifying any living person who is infringing their copyright by means of the settlement and protocol. I do not regard it as at all likely that they will attempt in any way to use the IP address as supplied to them by DtecNet of those engaged in illegal downloading in order to find out their names and addresses. Further, since, on the affidavit evidence before me, the plaintiffs had previously engaged in expensive litigation against Eircom in order to find out who they were, there seems no legal avenue open to them to get that information apart from an application for the names and addresses of the copyright thieves to the internet service provider. It is proved to me to be close to impossible that they could have recovered them by any easier or less pricey means. Nor do any of the plaintiffs have any intention of engaging in any illegal activity. Rather, the entire purpose of this litigation is to uphold the law. The first question is therefore answered no.

Issue 2

26. The second issue raised by the Data Protection Commissioner questions whether the settlement furthers any

legitimate interest pursued by Eircom and asserts a possible conflict with the fundamental rights and freedoms of the data subject. For the sake of clarity, I reproduce it again:

> "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"?

27. I define this issue as involving, firstly, identifying if there is a necessity from the point of view of Eircom in entering into the settlement. Secondly, it is relevant whether there is any right to steal somebody else's copyright material. Thirdly, and in the context of the first two questions, it is relevant to ask if the protocol involves any interference with any fundamental right or freedom involving internet service. If so, I must consider any intervention on the basis that the interference should be proportional and justified. This involves, in this context, looking at what is protected; how important that right is; what level of threat is directed at that right; and what level of participation may be legitimately inferred against the data subject. Since this question is responsibly based by the Data Protection Commissioner on s. 2A of the Act as amended I need to quote that in full:

> "2A(1) Personal data shall not be processed by a data controller unless section 2 of this Act (as amended by the *Act of 2003*) is complied with by the data controller and at least one of the following conditions is met:
>
> (a) the data subject has given his or her consent to the processing or, if the data subject, by reason of his or her physical or mental incapacity or age, is or is likely to be unable to appreciate the nature and effect of such consent, it is given by a parent or guardian or a grandparent, uncle, aunt, brother or sister of the data subject and giving such consent is not prohibited by law,
>
> (b) the processing is necessary –
>
> (i) for the performance of a contract to which the data subject is a party.
>
> (ii) in order to take steps at the request of the data subject prior to entering into a contract.
>
> (iii) for compliance with a legal obligation to which the data controller is subject other than an obligation imposed by contract, or
>
> (iv) to prevent –
>
> (I) injury or other damage to the health of the data subject or
>
> (II) serious loss or damage to property of the data subject,
>
> or otherwise to protect his or her vital interests where the seeking of the consent of the data subject or another person referred to in paragraph (a) of this subsection is likely to result in those interests being damaged.
>
> (c) the processing is necessary –
>
> (i) for the administration of justice,
>
> (ii) for the performance of a function conferred on a person by or under an enactment,
>
> (iii) for the performance of a function of the Government or a Minister of the Government, or
>
> (iv) for the performance of any other function of a public nature performed in the public interest by a person.
>
> (d) the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject".

28. In dealing with this aspect of data protection entitlement, I feel I must return, for a moment, to some basic principles of law. There is fundamental right to copyright in Irish Law. This has existed as part of Irish legal tradition since the time of Saint Colmcille. He is often quoted in connection with the aphorism: le gach bó a buinín agus le gach leabhar a chóip (to each cow its calf and to every book its copy). I regard the right to be identified with and to reasonably exploit one's own original creative endeavour as a human right. Apart from legal tradition, the rights now enshrined in the Copyright and Related Rights Act, 2000 were, under their previous legislative incarnation, identified in *Phonographic Performance Ireland Limited v. Cody*, [1998] 4 I.R. 504 by Keane J. at 511 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."

29. I regard that authority as both binding and sound. The courts under the Constitution are obliged to supply, even in the absence of legislative intervention, appropriate remedies for the undermining of rights within the scheme of fundamental law that the Constitution represents. As has often been said, the powers of the courts in that regard are as ample as the Constitution requires. I am, therefore, obliged by Constitutional imperative to protect, as best I can, the rights of copyright owners from unjust attack or, where that sort of attack has taken place, to vindicate their rights through an appropriate order. There is ample expression of statutory remedies in the laws passed by the Oireachtas under the Constitution. Section 37 of the Copyright and Related Rights Act 2000 provides that the owner of the copyright in work has the exclusive right to undertake or authorise others to make that work available to the public. This legal entitlement is being flagrantly violated by peer-to-peer illegal downloading. I can see no other way of looking at the problem. More than one of the conditions in s.2A of the Data Protection Act 1988 as amended is met as to both the legitimate interests of Eircom, as a responsible company, and that of the community in general. The most important of these interests is that of abiding by the law. It is completely within the legitimate standing of Eircom to act, and to be seen to act, as a body which upholds the law and the Constitution. That is what the court expects of both individuals and companies. That expectation is derived from the rights protected under the Constitution and the general pact which the people of Ireland mutually made in founding a legal system, as the Preamble to the Constitution clearly declares, that is dedicated to attaining true social order. The insertion of express conditions by Eircom in the user – internet service provider contract, as quoted above, against the use of the internet as a facility for transmitting obscene images and against the infringement of the copyright of others is a step taken in pursuance of a corporate policy that is no less than lawful and proper. It is abundantly clear that the data subject has given his or her consent in return for obtaining internet access. Under contract, if any of these conditions be breached, then their access can be terminated. It may be that internet access is available elsewhere from other internet service providers on lesser conditions. If that is so it is hard to see, however, how conditions of a contract can validly avoid the law. These, however, are the conditions that apply here. A contract for service, involving termination for breach as a consequence on the operation of a condition is present by consent. That is not all. Furthermore, such processing, involving sifting the data from the plaintiffs, warning Eircom customers and, ultimately, cutting them off, is necessary for both the performance of a contract and for compliance with a legal obligation cast upon the courts, among other organs of the State, to defend the Constitution and the laws of our society. No one in the community can escape the law, as to the obligations that it imposes or the rights that it declares. The means of infringement, or the ideology that may grow around a medium of infringement, are not germane. Otherwise, the law lacks legitimacy.

30. Even if only s. 2A(1)(b) of the Data Protection Act, as amended, was operative, it is legitimate for Eircom to have a corporate policy whereby the facilities that it hires out to the people of Ireland are used for lawful purposes only. Having that policy, they are entitled to pursue it by means of conditions in contract that incorporate an enforcement modality. The protocol is merely a more complex means to that end. I find it impossible to imagine that such interference is unwarranted because there is some fundamental right or freedom or legitimate interest in the data subject whereby, in contrast to those who engage in other forms of unlawful copyright theft which may leave them more readily subject to the law, the internet is used for the violation. There cannot be a right to infringe the constitutional rights of others, absent some argument as to a genuine and compelling competing right. In some instances, the purpose for which a right is asserted undermines its character as a right. There could not be, for instance, a constitutional right to privacy that extended to the organisation of a violent crime over the internet or by telephone. There is nothing disproportionate, and it is therefore not unwarranted, about cutting off internet access because of three infringements of copyright. The exceptions in the protocol, to which I have already referred in detail, provide for upholding relevant rights to medical care, to livelihood and to business use in appropriate circumstances. The protocol, at the relevant stage, is not inhumane or arbitrary. Rather, there is a right to make representations and these will, I am assured and I believe, be listened to if sensible and credible.

31. These are adequate procedural safeguards in the protocol and there is conformity, in addition, in my view, with article 1(b) of the European Parliament and Council Directive 2009/140/EC of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services O.J. L 337/37 18.12.2009, commonly called the framework Directive. At the moment there is no instrument making this effective in Irish law, but I have been referred to it as a matter of caution.

32. Lastly, I note the many Directives in European Law on the harmonisation of aspects of copyright and related rights. The Copyright and Related Rights Act 2000, as amended by the Copyright and Related Rights (Amendment) Act 2007 is a domestic Act, but it must be interpreted in accordance with Ireland's obligations under European law. In part, some terms are derived from our European Union obligations. The relevant European law Directives were implemented piecemeal over many years and later Directives, at times, repeat the text of earlier ones. Two sections of the European Parliament and Council Directive 2001/29/EC of 22nd May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society O.J. L167/10 22.6.2001 are important. Firstly, recital 59 records:-

> "In the digital environment, in particular, the services of intermediaries may increasingly be used by third parties for infringing activities. In many case 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."

33. And then there is Article 8.3 of the Directive:-

> "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".

34. In the Copyright and Related Rights Acts 2000, as amended, references to the right of the copyright holder in section 40 to make available to the public copies of a work are declared to include such acts as broadcasting the work, issuing copies of it or renting out copies; as in DVD libraries. Then, after establishing those legal entitlements in the holder of copyright, subs. 3 and 4 of that section go together and I quote them:-

"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."

35. Injunctions are granted by the court where it "just and convenient". That is the basis for all equitable relief formalised by the Supreme Court of Judicature (Ireland) Act 1875. I interpret the Copyright and Related Rights Act 2000 as extending to the making of an injunction against an innocent third party in order to block, in the appropriate way that is convenient as to the balance between the parties and that is just, as to their standing and conduct, the wholesale illegal destruction of the right to livelihood through creative effort which copyright, as a fundamental concept in law, is designed to defend and to vindicate. I make no comment on the protection of rights through injunctive relief where a primary actionable wrong in damages is not present; see *Prince Albert v Strange* (1849) 2 De & Sm 293 and, more recently, *Douglas v Hello!* [2002] 2 A.C. 457. The second question should therefore be answered no.

Issue 3

36. Central to this two-part third issue raised by the Data Protection Commissioner is whether the processing by Eircom, through warning and then on the third infringement, through cutting internet access, involves sensitive personal data. It admits of only one answer. I, again for clarity's sake, requote the issue:

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

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."

37. In considering this issue, I recall that since the earliest days of entitlement to copyright as enshrined in legislation, it has been both part of the civil code of law and it has also involved the creation of a number of criminal offences. These criminal offences are now set out in s. 140 of the Copyright and Related Rights Act 2000. I need to quote this in part:-

"140(1) A person who, without the consent of the copyright owner

(a) makes for sale, rental or loan,

(b) sells, rents or lends, or offers or exposes for sale, rental or loan,

(c) imports into the State, otherwise than for his or her private and domestic use,

(d) in the course of a business, trade or profession, has in his or her possession, custody or control, or makes available to the public, or

(e) otherwise than in the course of a business, trade or profession, makes available to the public to such an extent as to prejudice the interests of the owner of the copyright,

a copy of a work which is, and which he or she knows or has reason to believe is, an infringing copy of the work, shall be guilty of an offence…

(7) A person guilty of an offence under subsection (1) … shall be liable-

(a) on summary conviction, to a fine not exceeding £1,500 in respect of each infringing copy, article or device, or to imprisonment for a term not exceeding 12 months, or both, or

(b) on conviction on indictment, to a fine not exceeding £100,000, or to imprisonment for a term not exceeding 5 years, or both".

38. These are certainly criminal offences but they are not merely regulatory offences, the commission whereof may involve no element of mental culpability beyond doing the action outlawed. They are true criminal offences. They involve an external element of the infringement of copyright, in one of the modes provided for; an absence of any consent of the copyright owner; and a mental element of knowing or having reason to believe that one is dealing with an infringing copy of the work: in other words knowledge or recklessness. I am satisfied that neither the plaintiffs as owners or assignees of valuable copyright, nor Eircom as the internet service provider, are in any way interested in the detection or prosecution of criminal offences. There are now many instances where civil liability and criminal responsibility coincide by reason of statute. The most obvious example occurs under the Taxes Consolidation Act, 1997 whereby every infringement of taxation regulation is made into a crime. Every statutory instrument of which I am aware under the European Communities Act 1972, as amended, involves an apparently fixed policy of transmuting European law Directives into Irish law in a form that makes an infringement of the relevant term a summary offence. The Act forbids the creation by statutory instrument of indictable offences. Even before that modern statutory tendency, matters such as assault and false imprisonment

existed in virtually identical form in tort law and in criminal law by virtue of accepted common law definitions carrying remedies, on the one hand, in damages and, on the other, in punishment.

39. There doesn't seem to be any relevant issue, however, as to any mental element for the proof of any relevant criminal offence in terms of the purpose in processing data that is dependent upon the legal definition of sensitive personal data contained in the definition section of the Data Protection Act 1988, as amended. I quote this:-

> "Sensitive personal data means personal data as to
>
> (a) the racial or ethic origin, the political opinions or the religious or philosophical beliefs of the data subject,
>
> (b) whether the data subject is a member of a trade union,
>
> (c) the physical or mental health or condition or sexual life of the data subject,
>
> (d) the commission or alleged commission of any offence by the data subject, or
>
> (e) any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in any such proceedings."

40. In consequence, it could be argued that the sensitivity of data in relation to crime is centred on the commission of the offence, or an allegation of the commission of an offence through criminal process. That could be a parking offence or a litter offence as well as arson or murder. But, criminal proofs as regards the definitional elements of the first two offences differ markedly from the last two. This much, however, is obvious. Nothing in the affidavits that I have seen, nor anything in the evidence which I have heard, shows any interest by any of the plaintiffs, much less by the defendant, in alleging the commission by the person illegally downloading copyright material, the data subject, of a criminal offence. Nothing in the protocol to which I have referred will ever involve "the disposal of… proceedings" or "the sentence of any court". This strikes me as having high relevance to the third issue. Furthermore, since one is dealing here not with a regulatory offence, one which carries no necessary mental element of culpability, but with a true criminal offence, which does, there is nothing in the terms of the settlement, or the resulting protocol, or the attitude of the parties, which is directed at that crucial, and elusive, proof of the relevant mental element in criminal law. Rather, everything that I have seen is based upon civil law principles. In contrast to the criminal process, these establish liability by virtue of the proof of external facts, without any necessity to proceed to look to knowledge or intention, to recklessness or to criminal negligence (an element exclusive to manslaughter not relevant here). Even in the law of negligence, one is concerned with what ought to have been realised or done and not, as in criminal law, with what was perceived. As to the principles of liability, civil and criminal law are entirely different.

41. I do not believe that, in truth, this issue arises at all. Nor do I believe that it is necessary that there should be an investigation by an authorised body, or a determination made by a court of competent jurisdiction, following the conduct of a fair and impartial hearing, in order to determine that an offence has in fact been committed. That is because, in reality, no one is accusing anyone of an offence. There is no issue as to anything beyond civil copyright infringement. To accuse them of the criminal offence it would have to be copyright infringement together with the mental element expressly required by the crime.

42. In the course of the hearing, as I have said, reference was made to the framework directive, Directive 2009/140/EC. Its seems to me that the right to an effective and timely judicial review can be enabled by the State, if following settlements as carefully drafted as the protocol to which I have referred, or injunctions granted by the court in accordance with s. 40(4) of the Copyright and Related Rights Act 2000 as interpreted in accordance with Article 8.3 and recital 59 of the Directive 2001/29/EC, that an overall supervisory review of a settlement can in future be made at the time by the court granting an injunction or other order with all due respect to fundamental rights and freedoms. Any of that is an aspect of the future regulation of a very serious problem. As it is, I believe that I have made that review now and that nothing prevents the Court from enforcing the orders made in the settlement. The answer to the last composite question is therefore yes, the graduated response process is lawful. As to the present, I believe I have answered the questions posed as best I can.

Result

43. The parties can therefore lawfully proceed to implement the settlement.