Neutral Citation Number: [2012] IEHC 264

The High Court

Commercial

Judicial Review

[2012 No. 167 JR]

Between

EMI Records (Ireland) Limited

Sony Music Entertainment Ireland Limited

Universal Music (Ireland) Limited and

Warner Music Ireland Limited

applicants

and

The Data Protection Commissioner

respondent

and

Eircom plc

notice party

Judgment of Mr Justice Charleton delivered on the 27th day of June 2012

1.0 On Sunday 28 March 2010 all clocks in Ireland and around Europe went forward one hour at 01.00 hours for summer time. On Sunday 31 October 2010 all clocks in Ireland and Europe went back one hour at 02.00 hours for winter time. Eircom plc, the notice party and a major telecommunications and internet service company, ignored the winter time change. That piece of indolence led to this case.

1.1 For about the previous four months, from August 2010, Eircom had been operating a scheme under a settlement in a prior copyright infringement case whereby the plaintiffs in this case, hereafter referred to as the recording companies, were detecting on the internet those who were uploading their copyright in music and video; they then passed on information consisting only of copyright title, time and temporary IP address to Eircom. That company would then write to their subscribers and remind them that under the Eircom-subscriber contract they had agreed not to use internet access to infringe copyright. As was well publicised after that earlier litigation, after three such infringements the subscriber would lose a week of internet access and, after four, internet service from Eircom would be withdrawn altogether. This would not stop a subscriber seeking service from another internet service provider, of which there are more than a dozen in the State. Such information as to who might be deprived of internet service by any internet service provider is not put on any national register nor is there any equivalent collective internet service provider database.

1.2 Internet Protocol ("IP") addresses are furnished in their millions by a central agency called Réseaux IP Européens ("RIPE"), an organisation based in Paris, to internet service providers. On subscribing for internet service, a customer gets a router box from a provider and this has a unique number known only to the parties to that contract. Day by day, providers assign IP numbers to their subscribers and these typically change every 24 hours. The Court was told that some large companies like to have a more lasting IP address, but there is no evidence of that here. When a subscriber uploads or downloads a track without copyright permission on a peer-to-peer swarm of internet users, a file hash attaches to each piece of the track and this has attached to it that temporary IP number. In Ireland, the recording companies, through an agency, are on the internet joining swarms and detecting any IP addresses that are uploading copyright material assigned by artists to them. Where an Eircom IP address appears, that agency notifies Eircom on behalf of the recording companies and pursuant to the agreement between the parties, the subscriber is identified by Eircom and is written to. At no stage do the recording companies know to whom that IP address was assigned on any particular day and at no stage do they seek to gain that information from Eircom. Rather, any step that is thereafter taken remains confined to the privacy of the internet service provider and subscriber contract.

1.3 When Eircom did not change its clocks for a period of months from October to December 2010, some 391 subscribers were notified in the wrong that they had uploaded copyright material in breach of contract. On 9 December 2010, one particular subscriber received a contract breach notification incorrectly. On 17 January 2011, that subscriber wrote to the Data Protection Commissioner, the respondent herein. Correspondence then ensued with Eircom. That company acknowledged that a mistake had been made. The clocks were changed. On being informed of this, the particular made an additional complaint that a breach of privacy had occurred in that no permission had been given to the recording companies to monitor his internet activity; even though they had not done so in fact since that subscriber had never uploaded copyright material. The subscriber complained that there was an ongoing breach of data protection law and requested that "action is taken against Eircom … to the fullest extent of the law".

1.4 Action was indeed taken. As to whether it was lawful is the issue in this judicial review. By a notice dated 11 January 2012, Eircom was directed by the Data Protection Commissioner to cease its scheme with the recording companies.

Issues
2.0 There are three arguable issues in this judicial review. First, is judicial review available to the recording companies notwithstanding that a statutory appeal is open to Eircom against this decision of the Data Protection Commissioner? Second, have reasons been given in the notice? Third, is the notice incorrect in law or is it, instead, issued under an error of law that is in excess of jurisdiction?

2.1 A complicating issue in this judicial review, which would ordinarily be a simplifying factor, is that the subject matter of the notice was dealt with in a previous judgment of the Court, namely: EMI Records (Ireland) ltd v Eircom Ltd [2010] 4 IR 349. The Data Protection Commissioner makes a number of points in argument. In respect of the earlier judgment, he says that he was not present, and he was not because he declined to participate citing cost as the factor; he says that his absence from the case was not his fault; he says that the judgment does not bind him; he says that the Court was wrong in the judgment in which he deigned not to participate; he argues that the law has changed since that decision was delivered; he says he has given reasons for his decision in the notice; he says that if he did not, the reasons were obvious; he says that people should come and talk to him; and he says that he is not obliged to give advice to those who might come and talk to him.

2.2 The Court gave the recording companies, Eircom and the Data Protection Commissioner the option of stating questions in this case to the Court of Justice of the European Union. All declined. This judgment is subject to an appeal to the Supreme Court. The Court is entitled to stay any order that can be stayed to allow any party to exercise the option of appeal.

History
3.0 In 2005, Kelly J granted the recording companies a number of disclosure orders against Eircom. These related to IP addresses of the infringers of their copyright. Proceedings were initiated against some of those infringers. The practice proved to be futile in terms of general impact on the level of infringement; since each party was entitled to costs as in a third party discovery, the level of costs was completely out of proportion. The High Court later so held. In 2008 the recording companies took a case against Eircom seeking injunctive relief in part motivated by concerns as to whether a company could use a technical solution to block or divert or interrupt internet users who were acting in breach of copyright. During the course of that hearing Prof Leonard Kleinrock, one of the founders of the internet, gave evidence on behalf of the recording companies. At the conclusion of his evidence, the parties adjourned and returned with a settlement to the Court. That settlement involved what has been termed the graduated response, or three strikes, protocol. That protocol was filed in Court on 29 January 2009. It has since been altered into the form previously described herein. Part of the settlement terms was that Eircom would not oppose an application to block access to The Pirate Bay website through which much of the peer-to-peer downloading which infringed copyright was facilitated. That injunction application occurred before the Court and the emphasis was on European directives which require a remedy by way of injunction. An injunction requiring Eircom to block access to The Pirate Bay was then granted on hearing only the recording companies' side of the case. In fact, European law gave a power to grant such an injunction but that power had not been transposed into Irish law. Another part of the settlement was that the recording companies would pursue the other internet service providers for injunctive relief. The recording companies thereafter issued proceedings against all other internet service providers.

3.1 Meanwhile, the Data Protection Commissioner had become involved in discussions with Eircom over the period 11 May 2009 to 17 December 2009 specifically concerning the settlement and the protocol. He was concerned about three specific questions. At his request, Kelly J re-entered the case so that data protection issues could be decided by the High Court. The Data Protection Commissioner set out a list of the three questions on which he had concerns. Notably, he did not set out any other issues including ones which are now the subject of the notice in question in this case and notwithstanding the fact that those issues existed in law at that time, albeit under a different format. On 15 January 2010 the Data Protection Commissioner wrote a formal letter to Eircom as to his concerns. These issues were fixed by Kelly J for hearing. The Data Protection Commissioner sought an assurance in advance of the hearing that the parties would pay for his costs and/or would not seek costs against him. When that assurance was not forthcoming he declined to appear at the hearing because, he said, he was not funded for that role. It is obvious that the Data Protection Commissioner, having an important role by statute, ought to be properly and appropriately funded to take part in litigation that is central to the functions of his office. It is wrong that he was not so funded by those responsible. On 16 April 2010, having heard the parties attending, this Court gave judgment on the data protection issues. In August 2010 the protocol commenced. Meanwhile, the recording companies had issued proceedings against UPC, another major internet service provider. That case did not settle but was decided by the High Court.

3.2 On 11 October 2010 this Court gave judgment declining to grant injunctive relief to the recording companies, see EMI Records (Ireland) Ltd & Ors v UPC Communications Ireland Ltd [2010] IEHC 377. The reasoning of the Court was straightforward. Section 40(4) of the Copyright and Related Rights Act 2000 provides that where an owner of copyright notifies a party who makes available facilities for enabling the making available to the public of copies of a work "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." At the time of the passing of the Copyright and Related Rights Act 2000, Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce in the Internal Market ("E-Commerce Directive") had been passed. Article 22 of that directive gave the State up to 17 January 2002, to implement its terms. The Copyright and Related Rights Act 2000 was passed in light of draft legislation and in anticipation of what would become Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2011 on the harmonisation of certain aspects of copyright and related rights in the information society ("Copyright Directive"). Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services ("Framework Directive") was passed on 7 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). Article 14 of the E-Commerce Directive provides, at subpara. 3, that the defences described in that article are not to prevent a court, in accordance with the Member State's legal systems, from requiring "the service provider to terminate or prevent an infringement". A similar wording is contained in other directives. The wording used in the European directives refers to interruption, diversion and blocking. In particular, Recital 46 of the E-Commerce Directive provides that: "… upon obtaining actual knowledge or awareness of illegal activities [the internet service provider] has to act expeditiously to remove or to disable access to information …". The E-Commerce Directive has specific reference to the possibility of an injunction in Recital 45:

The limitations of the liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds; such injunctions can in particular consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it.

3.3 Article 12, entitled "Mere Conduit", imposes the following obligation on Member States:

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.

3.4 The process described in the European legislation is not the same as removing infringing material, which is the wording under section 40(4) of the Copyright and Related Rights Act 2000. An intermediary is not removing a music or video track by blocking or diverting it when it is shooting along an electrical connection in tiny pieces from many sources. To stop copyright infringement, an intermediary needs to terminate or disable or prevent the communication. In turn, that depends on the relevant technical solution proposed in litigation. The European legislation words are: remove, disable, terminate, prevent. When a legislature uses different words in legislation, the canons of statutory construction indicate that different concepts are generally referenced in respect of the use of each word. After that judgment, the recording companies issued proceedings against the State for failure to implement European law resulting in a direct loss to them. A regulation was passed which supposedly corrected the legal deficit. This regulation was accompanied by statements from an official of the relevant department of Government that the legislation did not in fact have the defect identified. This does not matter. A court decision is open to respectful criticism under the Constitution. The recording companies, however, which had a pressing imperative to enforce copyright, did not appeal that judgment; surprising if the judgment was wrong.

3.5 The three questions asked by the Data Protection Commissioner in the proceedings inspired by him, but in which he did not participate, were:

1. Does data comprising IP addresses, in the hands of the plaintiffs or their agent(s), and taking account of the purpose for which they are collected and their intended provision to the defendant, constitute 'personal data' for the purposes of the Data Protection Acts 1988 and 2003, thereby requiring that the collection of such IP addresses by the plaintiffs or their agents must comply with the specific requirements of each of ss. 2, 2A, 2B, 2C and 2D of the Data Protection Act 1988, as amended?

2. Having regard to s. 2A(1) of the Data Protection Act 1988, as amended, and assuming for current purposes that the processing by the defendant of "personal data" in the context of the third of the 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 the defendant", does such 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 ss. 2A(1) and 2B(1) of the Data Protection Act 1988, as amended, is it open to the plaintiffs and/or the defendant 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;

(b) the termination of an internet user's subscription by the defendant 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.

3.6 The answers of the Court given in the absence of the Data Protection Commissioner are available at [2010] 4 IR 349, at 361-373.

3.7 In defence of this application to quash the notice of 11 January 2012, counsel for the Data Protection Commissioner submits that: the relevant legislation has since changed, that is correct but he accepts that the legislation was there in similar form previously; that matters have moved from the theoretical to the practical with the complaint; that the Eircom contract with its subscribers should have been changed but was not changed, a matter that could previously have been argued by the Data Protection Commissioner but was not; that privacy law has been breached; and that the case law of the Court of Justice of the European Union has developed so as to make the prior judgment of the Court on data protection issues now irrelevant. The case apparently referred to in correspondence by the Data Protection Commissioner as changing the entire legal landscape on copyright protection was Case C-70/10 Scarlet Extended v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM).

The Notice

4.0 The notice of 11 January 2012 by the Data Protection Commissioner stated that the provisions of data protection legislation infringed by Eircom through the settlement and protocol were:

1. Regulation 5(1) of the Regulations in that eircom has facilitated or is facilitating the listening, tapping, storage or other kinds of interception or surveillance of communications and related traffic data of users of eircom's internet services, by persons other than such users, without the consent of the users concerned by means of implementing the Protocol;

2. Regulation 6 of the Regulations in that eircom has failed (or is failing) to ensure that traffic data relating to subscribers and users processed and stored for the purpose of the transmission of a communication (including, in particular, traffic data comprising IP addresses assigned by eircom to a subscriber at a particular point in time) is erased or made anonymous when it is no longer needed for that purpose save to the extent that such data may be retained and processed and/or stored for a purpose prescribed in the Regulations;

3. Sections 2(1)(a) & 2D of the DP Acts in that eircom has failed (or is failing) to provide subscribers with information necessary to render the obtaining and/or processing of their personal data "fair" for the purposes of said Section 2(1)(a).

4. Section 2(1)(b) of the DP Acts in that eircom has failed (or is failing) to comply with the requirement that personal data obtained and/or processed by or on behalf of eircom shall be accurate, eircom having incorrectly identified particular subscribers as persons who had engaged in illegal peer to peer file sharing using IP addresses assigned to eircom;

5. Section 2(1)(c)(i) of the DP Acts in that eircom has obtained (or is obtaining) personal data in respect of subscribers other than for one or more specified, explicit and legitimate purposes;

6. Section 2(1)(c)(ii) of the DP Acts in that eircom has further processed (or is further processing) personal data in respect of subscribers in a manner incompatible with the purpose for which that data was obtained and is retained;

7. Section 2A(1) of the DP Acts in that eircom has processed (or is processing) personal data of a subscriber without the subscriber's consent and/or without meeting any one or more of the other conditions specified in that Section;

8. Section 2B of the DP Acts in that eircom has processed (or is processing) sensitive personal data, namely data relating to the commission or alleged commission of offences further to Section 140 of the Copyright and Related Rights Act 2000, without complying with the requirements of Sections 2 and 2A of the DP Acts and/or without meeting one or more of the conditions specified in Section 2B(1)(b) thereof.

4.1 The Data Protection Commissioner therefore ordered, on peril of the commission of a criminal offence, that Eircom bring the implementation of the protocol to an end by taking the following actions:

(i) take all such steps as are necessary to comply with the provisions of the DP Acts and Regulations concerned, such steps to be taken within 60 days of the date of receipt of this Notice;

(ii) pending such steps being taken, to cease forthwith the obtaining and/or processing of subscriber data in the context of the implementation of the Protocol, including, for the avoidance of doubt, the receipt of subscriber data from, or the transmission of subscriber data to, any other party to the Protocol or their servants or agents; and,

(iii) take steps to destroy and/or erase any and all subscriber data processed by eircom in the context of the implementation of the Protocol within 60 days of receipt of this Notice.

4.2 It is with a degree of concern that the Court immediately notes that the Data Protection Commissioner does not accept that the mistake by Eircom in adjusting clocks was then in the past. It is neither legally right nor fair that an error can give rise to a command over a year later to cease an activity when that error has long since been corrected and where there is no indication that it would ever be repeated.

Curial deference

5.0 Only in defined circumstances is judicial review of a decision-making process available. To extend judicial review outside the proper boundaries of that remedy is to introduce uncertainty into the interaction of judicial and administrative power; see Efe v Minister for Justice, Equality and Law Reform [2011] IEHC 214. There can be tribunals which of their nature deal with specialist disciplines. Where questions of the balance of policy in specialist areas, or findings of fact requiring expert assessment, are concerned, then the courts should not readily find that findings of fact are irrational or that the balance struck between competing interests fails to accord with fundamental commonsense; this is the ordinary reasonableness test but one which in respect of a specialist tribunal a court should show appropriate deference. Such specialist tribunals, however, remain obliged to stay within the jurisdiction which statute has conferred on them and are required to make their assessments on considering both sides of an issue in an appropriate way and to furnish their decisions with reasons when statute or the appropriate inference from statute so requires. Curial deference does not aid such a specialist tribunal beyond according due respect for its expert factual assessment or decision on the balance of competing interests. Curial deference cannot extend to sanctioning breaches of the rules as to jurisdiction or the bypassing of the tribunal of the obligation to incorporate fair procedures. To so regard some tribunals would be to operate a discriminatory system of judicial review. In Frank Harrington Ltd v An Bord Pleanála [2010] IEHC 428 at paragraph 7.1 Hedigan J is not to be taken as extending curial deference outside the appropriate boundaries when he said:

When judicially reviewing a decision of an expert body the courts must exercise an appropriate measure of restraint. The nature of Judicial Review of expert bodies was addressed in Henry Denny & Sons (Ireland) Ltd. v. Minister for Social Welfare [1998] 1 I.R. 34. Hamilton CJ stated that:

"It would be desirable to take this opportunity of expressing the view that the courts should be slow to interfere with the decisions of expert administrative tribunals. Where conclusions are based upon an identifiable error of law or an unsustainable finding of fact by a tribunal such conclusions must be corrected. Otherwise it should be recognised that tribunals which have been given statutory tasks to perform and exercise their functions, as is now usually the case, with a high degree of expertise and provide coherent and balanced judgments on the evidence and argument heard by them it should not be necessary for the courts to review their decisions by way of appeal or judicial review."

The need for restraint has been helpfully explained in the following terms:

"While a court must not lose sight of its unique role in determining the legality of a public decision, there are sound reasons for the exercise of restraint in the application of the review principles. If the judges overreach, they commit the error which review has been designed to prevent: they abuse jurisdiction. And in doing so, there is a practical danger that they may end up being responsible for decisions which they are not, by training or experience qualified to make. Specialist bodies are established by legislation often because their members will have particular knowledge of their fields of activity. That knowledge may often not necessarily be imparted to or rest in a judge dealing with a

review application"; De Blacam, Judicial Review, Second Edition (Dublin 2009).

5.1 Curial deference is not a new concept and it is not to be automatically applied even to bodies dealing with issues of fact. In the context of a statutory appeal, in Philadelphia Storage Battery Co. v Controller of Industrial and Commercial Property [1935] IR 575 Kennedy CJ said at 593:

The Courts in England have, however, indicated very strongly that they will pay great attention to the decision of a specialist officer like the Controller. No doubt the degree of such attention will vary with the length of time he has held his office and his consequent experience, and the qualifications and the known ability of the officer. If the English courts went to the extent of accepting his view as the exercise of a judicial discretion by which the Court should be bound, we could not follow them in this country, as that would, in my opinion, be contrary to a constitutional principle which binds us, and which we must be jealous to maintain. In my opinion, therefore, while we read the views of the Controller with respect and in the present case with admiration of the clarity and ability of his statement of them, we are quite free to form our own opinion untrammelled by them.

5.2 It must be emphasised that curial deference cannot possibly arise where by statute reasons for a decision are required but none are given. Nor can curial deference ever be a factor in judicial review where a mistake of law puts a tribunal outside the jurisdiction conferred on it by statute. In appropriate cases, where errors occur even on those issues the general discretion as to judicial review may be invoked depending on the precise circumstances in appropriate cases. The principle of curial deference on issues of fact and decisions on the appropriate balancing of competing interests has, however, nothing to do with any case such as this one which concerns the obligation to give reasons for a decision and the proper interpretation of powers conferred by statute on an administrative official.

Peer-to-peer copying

6.0 A brief note as to how peer-to-peer copying works in the infringement of copyright is necessary. The parties agreed during the hearing that the evidence of Michael Walsh of the Irish consultancy firm, Kerna Communications Ltd, reproduced by Arnold J of the England and Wales High Court in Dramatico Entertainment Ltd and Others v British Sky Broadcasting Ltd and Others [2012] EWHC 268 (Ch) explained that process concisely and accuratly. This is the relevant extract from paragraph 19:

> … P2P services each differ from one another in many technical details, but they all share certain basic elements:
>
> (a) The user downloads and installs on his or her computer a piece of software, for example µTorrent (also known as uTorrent). This software is easily found using an internet search engine and is downloaded for free without any personal identification required.
>
> (b) Once the software is installed on a computer, whenever that computer connects to the internet it becomes part of a P2P network or system consisting of many other computers using the same software. P2P software often installs itself so that it runs in the background whenever the computer is started.
>
> (c) A user locates files for download in different places depending on the P2P technology in use. Bittorrent users may use The Pirate Bay because it is simple to search and find music, video, games and software.
>
> (d) Once a user is a participant in a P2P network, he or she can download files hosted and being made available by other users of the P2P network. At the same time the user's computer acts as an uploader, making the files that it has locally available to others. The files are not stored or hosted on a central server. Instead, each computer that is part of the network can act as a mini-server from which other P2P users on the network can download files.
>
> (e) P2P technology distributes large data files by breaking them up into small pieces (chunks) and sends them over the internet to the requesting user. The P2P software may request chunks of the file from different members of the P2P network. When all the data is received by the user's computer, the file is reassembled as a whole.
>
> (f) Because of their organisation, where users in a P2P network will generally act both as a client and a server (i.e. uploader as well as downloader), each participant provides resources to the network such as bandwidth, storage space and computing power, thereby increasing capacity as the network grows. P2P networks scale well as they grow in size and are resilient where there is no central component.

6.1 Prior to the enforcement notice of 11 January 2012, only two hints at any reasons behind that decision are contained in the Data Protection Commissioner's correspondence with Eircom. In so far as the questions that may have been concerning might be construed, these are issues as to privacy and issues as to a judgment of the Court of Justice of the European Union.

Privacy

7.0 Privacy is central to the arguments made by counsel for the Data Protection Commissioner. The Constitution of Ireland guarantees privacy as an unenumerated fundamental right under Article 40.3. Under Article 8 of the European Convention on Human Rights and Fundamental Freedoms, respect for privacy is guaranteed. Article 10 of the Convention also guarantees the right to communicate. The process of uploading copyright material involves engaging with a swarm as a participant from which and to which copyright material will be uploaded and downloaded. That activity can of course be lawful; as in uploading a television programme freely available on the website of a television company. Whether lawful or in breach of copyright, peer-to-peer uploading takes place openly on the internet in circumstances where the file hash will be accompanied by the temporary identification of the IP address, changing day by day (provided the clocks are properly set). Anyone can join such a swarm. In doing so for the purpose of uploading or downloading copyright material, that activity will be accompanied by an IP address which would mean nothing to uploaders and downloaders. That would not therefore identify anyone to any participant in the swarm. A specialist might be able to find out that such a number had been assigned by the Paris authority as one among hundreds of thousands to Eircom or to another internet service provider. Counsel for the Data Protection Commissioner likened the detection of an IP address by an agent of the recording companies participating in a swarm to that of university authorities opening the locker of, searching the home of and monitoring the mobile phone of students who have merely signed a contract for tuition. Such participation by an agent of the recording companies in a swarm that would not be for the purpose of illegal uploading and downloading but for the purpose of detecting those engaged in that activity, and that was to be equated, he argued, to the gardaí entering houses without a search warrant merely because they thought that there might be a controlled drug there. It was also to be assimilated to the criminal law defence of entrapment, he urged. Counsel for the recording companies submitted that everyone could think of people to whom they would wish to anonymously make threatening telephone calls but that desire did not render such activity either ethical or lawful. It is hard to agree with either of these submissions. Counsel for Eircom argued that the activity of peer-to-peer uploading and downloading of copyright material was a marketplace transaction which could not be distinguished from a trader going and standing on the side in Henry Street in Dublin city

centre with a box load of DVDs that were copied illegally and offering these to anyone who might come along. That submission is a fair characterisation.

7.1 Desiring that an activity remain undetected and having an entitlement to privacy are two entirely different concepts. Some activities are naturally private according to the notions of decent thinking. Sometimes the affairs that we share with others are private from the nature of what we communicate or the circumstances in which we share. Privacy may be described as the bundle of expectations held by reasonable citizens that actions which we legitimately shield from others, or communications in confidence, will be respected through not being enquired into as matters we are entitled to shield from others, or where communicated, disseminated outside the sphere within which the trust of others, arising through contract or the reposing of that trust, is expected not to be betrayed. Breach of privacy is thus the unwelcome intrusion of others into aspects of living that are particularly personal to the individual or into information shared in confidence. In Scarlet Extended, Advocate General Cruz Villalón appeared to endorse the idea that anonymity is essential for the preservation of what he called the right to privacy on the internet. In his opinion of 14 April 2011 at paragraph 73 he said:

> Il convient d'examiner successivement la mesure sollicitée en tant que possible limitation au droit à la protection des données personnelles, d'une part, et au droit au respect du secret des communications, d'autre part. 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 cyberespace. Cependant, s'il apparaît clairement que les directives 95/46 et 2002/58 doivent être interprétées au regard des articles 7 et 8 de la charte, lus le cas échéant à la lumière de l'article 8 de la CEDH, le lien unissant le droit à la protection des données personnelles (article 8 de la charte) et le déploiement du système de filtrage et de blocage sollicité est lui beaucoup moins clair.

7.2 In the judgment, the Court of Justice of the European Union did not rule on this proposition. That seems correct. An activity of swarm participation for peer-to-peer downloading does not legitimately carry the expectation of privacy. It is flying in the face of commonsense for the Data Protection Commissioner to equate participation in an open communication with all comers on the internet for the purpose of illegal downloading of copyright material with interception, with tapping or with listening. Those concepts are rightly to be deprecated as illegal in circumstances of privacy. That is not the situation here: there is no legitimate reposing of trust pursuant to contract or reasonable expectation that when a person goes on the internet with a view to uploading or downloading what does not belong to them. That circumstance does not give rise to any constitutional entitlement or human right to remain immune from a music company also participating in that open forum to discover the economic damage that is being done to it and to creative artists. The interest of music companies is proper and proportionate. It is beyond doubt that while each individual act of copying, in itself, does little damage the reproduction of that activity by millions repeated over time is industrial in scale. The response of internet service providers of doing nothing perhaps reflects the greater economic strength of intermediaries as compared to creative people or recording companies. There is also the immeasurable and disproportionate power of these peer-to-peer swarms which are increasingly rendering the entitlement to those on whom creativity depends to no consideration.

7.3 No evidence was offered in this case as to the application of privacy in these circumstances. Due to the lack of reasons in the notice of 11 January 2012, the motivation behind the condemnation by the Data Protection Commissioner of any music company participating, with a view to protecting its own interest in copyright, in a peer-to-peer swarm devoted to illegal uploading and downloading is not clear. Nor is it clear as to how privacy might come into the matter at all. This issue was analysed with the benefit of opposing argument and evidence by this Court in EMI Records (Ireland) Ltd & Ors v UPC Communications Ireland Ltd [2010] IEHC 377. I quote the appropriate paragraphs from that judgment:

> 66. The existence of a right to privacy is not in doubt; as Hamilton P. in Kennedy v. Ireland [1987] I.R. 587 put it, '[t]he right to privacy is not an issue, the issue is the extent of that right or the extent of that right "to be left alone". It has been consistently invoked in the courts over the years; see, for example, X v. Flynn (Unreported, High Court, Costello J., 19th May, 1994) and Re Article 26 and the Employment Equality Bill 1996 [1997] 2 I.R. 321. Despite this, privacy as a right is difficult to define adequately. The Irish courts have grappled with the scope of the right since it was first recognised in McGee v. Attorney General [1974] I.R. 284 as an unenumerated right, flowing from the State's undertaking to defend and vindicate the personal rights of every citizen under Article 40.3.1 of the Constitution. Privacy in the modern panoptic society must be flexible enough to address new technologies and developments and their privacy implications while at the same time certain enough as to offer guidance and clarity as a matter of law. Keeping this tension in mind, it is extremely difficult to arrive at an appropriate definition. Description is therefore preferable.
>
> 67. The right to privacy has been said to encapsulate the 'right to be left alone' (per Walsh J. in his dissenting judgment as a judge of the European Court of Human Rights in Dudgeon v. United Kingdom (1981) 4 E.H.R.R. 149) or as "the fundamental value of personal autonomy" (per Sedley L.J. in Douglas v. Hello! [2001] 1 Q.B. 967 at para. 126) – the right of the individual to exercise control over information, possessions and conduct of a personal nature and, as an obvious corollary, the right to prevent others from accessing this information. On an international level this State is a signatory to various treaties which clearly enumerate the right to privacy. The most important of these is contained in Article 8 of the European Convention on Human Rights which provides, inter alia, that "[e]veryone has the right to respect for his private and family life, his home and his correspondence". This right to 'be left alone' has spawned a considerable amount of data protection legislation, most noticeably at a European level (See, for example, Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data O.J. L 281 23.11.1995 ["the Data Protection Directive"]) and on a domestic level, principally through the Data Protection Act 1988, as amended.
>
> 68. I find it impossible to recognise as a matter of constitutional law, that the protection of the entitlement to be left in the sphere of private communications could ever extend to conversations, emails, letters, phone calls or any other communication designed to further a criminal enterprise. Criminals leave the private sphere when they infringe the rights of other, or conspire in that respect. Legislative intervention may mean detection involves a statutory infringement: leaving the admission of evidence to be decided on the balance of respect for the law and the seriousness of what is involved. In the case of internet file sharing to infringe copyright, I am of the view that there are no privacy or data protection implications to detecting unauthorised downloads of copyright material using peer-to-peer technology; (see, EMI Records (Ireland) Limited v. Eircom Limited [2010] IEHC 108, (Unreported, High Court, Charleton J., 16th April, 2010). In this regard, I am taking into account the fact that the process of detection through DtecNet is essentially anonymous. As previously emphasised, a communication between the recording companies and an internet service provider, having used the facilities offered by the DtecNet, that in a particular month a certain one hundred subscribers downloaded an average of twenty copyright protected tracks each, illegally, giving a date and time and the IP address, discloses no information publicly. The recording companies do not thereby harvest the names and addresses of infringers of copyright for data purposes, or for future communication or for evidence in a potential criminal case. They get nothing apart from a

set of numbers. As between UPC and their customers, any solution to this illegal activity is conducted privately as between them. They already know each other, as they are joined by a contract. That communication is within the range of matters over which an internet service provider is entitled to deal with its customer. The abuse of an internet service for copyright theft is a serious matter from the point of view of the general enforcement of copyright protection. An internet service provider is entitled to have a policy against it. In this instance, it is apparent that UPC pretends to have such a policy. The existence of a genuine anti-piracy policy would enhance the public standing of any corporation and is a matter in respect of which they have an interest. Enforcing a private contract, in this context, does not have privacy implications. Any form of blocking on that customer and internet service provider basis does not carry a privacy implication. If the response is a graduated one, as opposed to a blocking of communications merely on a basis of identifying its nature and the relevant IP number, no privacy implication arises. As Professor Nixon put it:-

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

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

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

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

7.4 Both experts in that case were of the view that privacy was not engaged by participating in a peer-to-peer swarm for detection purposes. A court cannot contradict such expert evidence. The keeping of billing information is argued by the Data Protection Commission to be unlawful. Counsel for Eircom pointed out that any commercial company facing a potential breach of contract action, which has a limitation period of six years, is entitled to keep and use billing information for that period. Furthermore by signing a contract which requires appropriate and lawful use of the internet, and specifically outlaws breach of copyright, the use of that billing information for enforcing a contract in the ordinary way is not inappropriate and does not constitute a breach of privacy. Apart from the fact that this issue could have been, but was not, raised by the Data Protection Commissioner in the previous litigation, contracts are to be construed in order to give business efficacy to that which has been agreed.

7.5 What is argued for here by the Data Protection Commissioner is that all of the contracts entered into by Eircom with its subscribers should be disavowed and a new contract circulated for acceptance or rejection on the basis of the protocol. Such a course would be unnecessary. The contract already contains the relevant clause and with it the clear implication that reliable information as to breach may be notified in a reasonable way to the relevant customers. If these subscribers find themselves in having to search out another internet service provider, that would occur only after four breaches of the copyright of others and in the context of having a full opportunity to offer an explanation and in the context of appropriate exceptions as to health and other important factors. I am not considering here any issue as to recourse to a judicial process before the termination of internet access between one individual subscriber and that subscriber's then internet service provider.

7.6 In summary, peer-to-peer sharing is no more a breach of privacy than any other form of participation in copyright infringement by any of the participants.

The Court of Justice of the European Union

8.0 The Court of Justice of the European Union has not authorised the unauthorised downloading of copyright material from the internet. To do so, the Court would have to reverse the relevant directives. Furthermore, any re-arrangement of fundamental rights to place copyright automatically at the mercy of competing rights to communicate, to run a business, to fair procedures or to privacy would, without any legal justification, place copyright as a lesser intellectual property entitlement to trade mark rights, to patent protection, to industrial secrets and to design protection. Copyright is not to be ranked above those entitlements. Nor, however, is there any warrant in European legislation or case decisions for any development that would place copyright below such entitlements, never mind outside legal protection, simply because breaches occur on the internet. In case C-324/09 O'Oréal v eBay the Court of Justice of the European Union affirmed that the infringement of trade mark rights online should give rise to an entitlement to an effective injunction against an intermediary at the suit of the holder of those rights. Intellectual property rights are at the heart of economic activity in the European Union. It was affirmed at paragraph 144 of the judgment that:

> …the third sentence of Article 11 of [Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights] must be interpreted as requiring the Member States to ensure that the national courts with jurisdiction in relation to the protection of intellectual property rights are able to order the operator of an online marketplace to take measures which contribute, not only to bringing to an end infringements of those rights by users of that marketplace, but also to preventing further infringements of that kind. Those injunctions must be effective, proportionate, dissuasive and must not create barriers to legitimate trade.

The relevant judgments all are to the same effect. Any decision to recast, much less to undermine, any form of intellectual property rights does not lie within the judicial sphere of government under the treaties.

8.1 In case C-275/06 Productores de Música de Espaòa (Promusicae) v Telefónica de Espaòa SAU, Promusicae, a non-profit body representing the interests of music and video producers and publishers, asked the relevant court in Spain for Telefónica to be ordered to disclose the identities and physical address of certain persons whom it provided with internet access and whose IP addresses and the date and time of their connection were known. Promusicae wanted to target users of a peer-to-peer file exchange programme, who it said were engaging in unfair

competition and the infringement of intellectual property rights. The first instance court granted the order sought. That order was appealed and a question referred to the Court of Justice of the European Union for a preliminary ruling. The question referred was:

> does Community law […] permit Member States to limit to the context of a criminal investigation or to safeguard public security and national defence, thus excluding civil proceedings, the duty of operators of electronic communications networks and providers of data storage services to retain and make available connection and traffic date generated by the communications established during the supply of an information society service?

The Court of Justice of the European Union ruled that Community law does not require the Member States to lay down an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings. However, it noted that, in transposing Directives 2000/31, 2001/29, 2004/58 and 2002/58, the Member States must take care to rely on an interpretation of them which allows a fair balance to be struck between the various fundamental rights protected by the European legal order. Finally, it reiterated that, when implementing the measures transposing those directives, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those directives, but must also ensure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of European law, such as the principle of proportionality. This analysis has not fundamentally changed and it does seem possible that it could change by judicial, as opposed to legislative, action. Each case is about the nature of the order sought to be imposed, the proportionality of that order to the burdens and benefits that it imposes and the balance to be struck between competing rights.

8.2 The Treaty on the Functioning of the European Union ("the Treaty") makes three specific references to intellectual property rights. Article 118 of the Treaty, which concerns the approximation of laws, provides that the European Parliament and the Council shall establish measures for the uniform protection of intellectual property rights throughout the European Union. Article 207 of the Treaty, which concerns the common commercial policy, explicitly provides that the common commercial policy shall be based on uniform principles which have regard for, inter alia, the commercial aspects of intellectual property. Finally, article 262 of the Treaty, which concerns the Court of Justice of the European Union, provides that the Court may be vested with the jurisdiction to resolve disputes relating to acts adopted under the treaties which create European intellectual property rights.

8.3 In case C-461/10 Bonnier Audio AB v Perfect Communication Sweden AB at issue was the interpretation of Articles 3 to 5 and 11 of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, and of Article 8 of Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights. This case was directly relevant to the issues which concerned the Data Protection Commissioner. At issue was a Swedish law which provided for disclosure of retained data from an intermediary where copyright infringement was sought to be pursued and where conditions of law entitled an author or a successor in title to apply to court. Such an order was not to be granted except under conditions of balancing the "nuisance or other harm which the measure entails for the person affected by it or for some other conflicting interest" and prevented disclosure that persons "close to him" had "committed a criminal act". Directly relevant was article 6 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). This law was in force when the Data Protection Commissioner first became involved in discussions on the settlement protocol in the EMI v Eircom case. This provides:

> 1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).
>
> 2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.
>
> 3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 1 to the extent and for the duration necessary for such services or marketing, if the subscriber or user to whom the data relate has given his/her consent. Users or subscribers shall be given the possibility to withdraw their consent for the processing of traffic data at any time …
>
> 5. Processing of traffic data, in accordance with paragraphs 1, 2, 3 and 4, must be restricted to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.
>
> 6. Paragraphs 1, 2, 3 and 5 shall apply without prejudice to the possibility for competent bodies to be informed of traffic data in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.

8.4 The Court of Justice of the European Union held that the relevant Swedish law conformed with the relevant directives and with the general principles of European law and that it struck an appropriate balance, or rather allowed the deciding judge to strike such a balance, between competing rights. Since there has been so much competitive argument on this case, the clarity of the reasoning of the Court provides a clear response:

> 51 In order to give a useful answer, firstly, it is necessary to bear in mind that the applicants in the main proceedings seek the communication of the name and address of an internet subscriber or user using the IP address from which it is presumed that an unlawful exchange of files containing protected works took place, in order to identify that person.
>
> 52 It must be held that the communication sought by the applicants in the main proceedings constitutes the processing of personal data within the meaning of the first paragraph of Article 2 of Directive 2002/58, read in conjunction with Article 2(b) of Directive 95/46. That communication therefore falls within the scope of Directive 2002/58 (see, to that effect, Promusicae, paragraph 45).
>
> 53 It must also be noted that, in the main proceedings, the communication of those data is required in civil proceedings for the benefit of a copyright holder or his successor in title, that is to say, a private person, and not for the benefit of a

competent national authority.

54 In that regard, it must be stated at the outset that an application for communication of personal data in order to ensure effective protection of copyright falls, by its very object, within the scope of Directive 2004/48 (see, to that effect, Promusicae, paragraph 58).

55 The Court has already held that Article 8(3) of Directive 2004/48, read in conjunction with Article 15(1) of Directive 2002/58, does not preclude Member States from imposing an obligation to disclose to private persons personal data in order to enable them to bring civil proceedings for copyright infringements, but nor does it require those Member States to lay down such an obligation (see Promusicae, paragraphs 54 and 55, and order in LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten, paragraph 29).

56 However, the Court pointed out that, when transposing, inter alia, Directives 2002/58 and 2004/48 into national law, it is for the Member States to ensure that they rely on an interpretation of those directives which allows a fair balance to be struck between the various fundamental rights protected by the European Union legal order. Furthermore, when implementing the measures transposing those directives, the authorities and courts of Member States must not only interpret their national law in a manner consistent with them, but must also make sure that they do not rely on an interpretation of them which would conflict with those fundamental rights or with the other general principles of European Union law, such as the principle of proportionality (see, to that effect, Promusicae, paragraph 68, and order in LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten, paragraph 28).

57 In the present case, the Member State concerned has decided to make use of the possibility available to it, as described in paragraph 55 of this judgment, to lay down an obligation to communicate personal data to private persons in civil proceedings.

58 It must be noted that the national legislation in question requires, inter alia, that, for an order for disclosure of the data in question to be made, there be clear evidence of an infringement of an intellectual property right, that the information can be regarded as facilitating the investigation into an infringement of copyright or impairment of such a right and that the reasons for the measure outweigh the nuisance or other harm which the measure may entail for the person affected by it or for some other conflicting interest.

59 Thus, that legislation enables the national court seised of an application for an order for disclosure of personal data, made by a person who is entitled to act, to weigh the conflicting interests involved, on the basis of the facts of each case and taking due account of the requirements of the principle of proportionality.

60 In those circumstances, such legislation must be regarded as likely, in principle, to ensure a fair balance between the protection of intellectual property rights enjoyed by copyright holders and the protection of personal data enjoyed by internet subscribers or users.

61 Having regard to the foregoing, the answer to the questions referred is that:

> Directive 2006/24 must be interpreted as not precluding the application of national legislation based on Article 8 of Directive 2004/48 which, in order to identify an internet subscriber or user, permits an internet service provider in civil proceedings to be ordered to give a copyright holder or its representative information on the subscriber to whom the internet service provider provided an IP address which was allegedly used in an infringement, since that legislation does not fall within the material scope of Directive 2006/24;
>
> it is irrelevant to the main proceedings that the Member State concerned has not yet transposed Directive 2006/24, despite the period for doing so having expired;
>
> Directives 2002/58 and 2004/48 must be interpreted as not precluding national legislation such as that at issue in the main proceedings insofar as that legislation enables the national court seised of an application for an order for disclosure of personal data, made by a person who is entitled to act, to weigh the conflicting interests involved, on the basis of the facts of each case and taking due account of the requirements of the principle of proportionality.

8.5 In the course of correspondence, the Data Protection Commissioner tersely mentioned that a recent decision, referring to Scarlet Extended by name, had changed the legal landscape and perhaps intended to imply that there had been a change of copyright protection for the reason that infringements of copyright were to occur on the internet. This attitude was described by counsel for Eircom as a startling misreading of that decision.

8.6 Case C-70/10 Scarlet Extended S.A. v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) involved a Belgian group called SABAM, representing authors, composers and publishers, initiating proceedings against an internet service provider called Scarlet. The group claimed an entitlement to a blocking order to bring to an end the illegal downloading of protected works by means of peer-to-peer use of the Scarlet server. The relevant Belgian legislation provided that where a third party uses the services of an intermediary to infringe the intellectual property of another, the courts can order the intermediary to bring the infringement to an end. In 2004, the President of the court of first instance found that copyright had been infringed and appointed an expert to assess the feasibility of the technical solutions proposed by SABAM. The expert identified one possible solution, namely CopySense produced by a firm called Audible Magic, but expressed reservations as to its capacity to deal with high volumes of traffic, the high acquisition and operating costs of the system and its potentially short technical duration of three years. The Court granted an injunction imposing that technical solution. On a referral of relevant questions to the Court of Justice of the European Union, Scarlet argued that the injunction would constitute a general obligation to monitor contrary to Article 15 of the E-Commerce Directive, that it would be contrary to the mere conduit defence in Article 12 of the E-Commerce Directive and, finally, that it would violate fundamental rights in particular the rights to privacy, confidentiality of correspondence and freedom of expression. From the text of the judgment, it is clear that the Court was concerned with the breadth of the injunction which it considered would impose on Scarlet a general monitoring obligation contrary to Article 15 of the E-Commerce Directive. Further, the Court did not consider that the order properly balanced the property rights enjoyed by the copyright owners against Scarlet's right to conduct its business. The Court was particularly concerned that the expense of installing the technology required would fall solely on Scarlet, contrary to Article 3 of the Enforcement Directive, which requires that remedies not be unnecessarily complicated or costly. The Court also considered that a filtering system would infringe the rights of Scarlet's users since it would involve the collection and identification of users' IP addresses contrary to Article 8 of the European Convention on Human Rights and could potentially lead to a blocking of lawful communications thus

undermining the freedom of information contrary to Article 11.

8.7 Very similar questions arose in another referral from the courts of Brussels to the Court of Justice of the European Union in Case C-360/10 Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV. This time the blocking order was sought against a social networking site. The injunction in question required what was described as "the installation of an expensive general monitoring system". That system seems also not to have been sufficiently tested. Such an order was a serious imposition on the hosting service provider's right to conduct a business. The Court held that it infringed the fundamental rights of the users to protection of their personal data and their freedom to impart information; in such circumstances, the rights of the copyright owners must give way. It is clear, however, from paragraphs 41 to 51 of the judgment that it is not at all in the instance of every application for an order to prevent copyright infringement that competing rights will require the refusal of an injunction in support of copyright:

The protection of the right to intellectual property is indeed enshrined in Article17(2) of the Charter of Fundamental Rights of the European Union ("the Charter"). There is, however, nothing whatsoever in the wording of that provision or in the Court's case-law to suggest that that right is inviolable and must for that reason be absolutely protected ...

As paragraphs 62 to 68 of the judgment in Case C 275/06 Promusicae [2008] ECR I 271 make clear, the protection of the fundamental right to property, which includes the rights linked to intellectual property, must be balanced against the protection of other fundamental rights.

More specifically, it follows from paragraph 68 of that judgment that, in the context of measures adopted to protect copyright holders, national authorities and courts must strike a fair balance between the protection of copyright and the protection of the fundamental rights of individuals who are affected by such measures.

Accordingly, in circumstances such as those in the main proceedings, national authorities and courts must, in particular, strike a fair balance between the protection of the intellectual property right enjoyed by copyright holders and that of the freedom to conduct a business enjoyed by operators such as hosting service providers pursuant to Article 16 of the Charter ...

In the main proceedings, the injunction requiring the installation of the contested filtering system involves monitoring all or most of the information stored by the hosting service provider concerned, in the interests of those rightholders. Moreover, that monitoring has no limitation in time, is directed at all future infringements and is intended to protect not only existing works, but also works that have not yet been created at the time when the system is introduced.

Accordingly, such an injunction would result in a serious infringement of the freedom of the hosting service provider to conduct its business since it would require that hosting service provider to install a complicated, costly, permanent computer system at its own expense, which would also be contrary to the conditions laid down in Article 3(1) of Directive 2004/48, which requires that measures to ensure the respect of intellectual-property rights should not be unnecessarily complicated or costly ...

In those circumstances, it must be held that the injunction to install the contested filtering system is to be regarded as not respecting the requirement that a fair balance be struck between, on the one hand, the protection of the intellectual-property right enjoyed by copyright holders, and, on the other hand, that of the freedom to conduct business enjoyed by operators such as hosting service providers ...

Moreover, the effects of that injunction would not be limited to the hosting service provider, as the contested filtering system may also infringe the fundamental rights of that hosting service provider's service users, namely their right to protection of their personal data and their freedom to receive or impart information, which are rights safeguarded by Articles 8 and 11 of the Charter respectively.

Indeed, the injunction requiring installation of the contested filtering system would involve the identification, systematic analysis and processing of information connected with the profiles created on the social network by its users. The information connected with those profiles is protected personal data because, in principle, it allows those users to be identified …

Moreover, that injunction could potentially undermine freedom of information, since that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications. Indeed, it is not contested that the reply to the question whether a transmission is lawful also depends on the application of statutory exceptions to copyright which vary from one Member State to another. In addition, in some Member States certain works fall within the public domain or may be posted online free of charge by the authors concerned ...

Consequently, it must be held that, in adopting the injunction requiring the hosting service provider to install the contested filtering system, the national court concerned would not be respecting the requirement that a fair balance be struck between the right to intellectual property, on the one hand, and the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information, on the other ...

8.8 A series of cases in England and Wales have made it clear that injunctive relief in aid of copyright protection on the internet can be granted in circumstances where there is a clear focus to the relief sought, unlike the unlimited order sought in Scarlet Extended, and where the balance of burdens and costs are proportionate. In Dramatico Entertainment Ltd and Others v British Sky Broadcasting Ltd and Others [2012] EWHC 268 (Ch) Arnold J described internet copyright infringement through the website The Pirate Bay, previously referenced in this judgment, as "vast in scale". When its founders, earning substantial revenues through online advertising, were convicted in Sweden on charges of criminal copyright infringement, they fled to other countries. Arnold J found that of the top 75 music albums available as of December 2011, 72 were available through The Pirate Bay. Access to that site was injuncted through the intermediaries of the main internet service providers in Britain. Part of the reasoning was that although they were conduits, authorisation of copyright infringement can occur where the action of the party charged goes beyond mere enablement, assistance or even encouragement. Participation occurs where there is a grant, or purported grant, of the right to do the tort complained of. This may be found on an analysis of the relationship between the alleged authoriser and the primary infringer; the equipment or other material supplied as a means to infringe; whether it was inevitable that such would be so used; the degree of control which the supplier retained; and whether that supplier had taken any steps to prevent infringement: see Kitchin J in Twentieth Century Fox Film Corporation & Ors v Newzbin Ltd [2010] EWHC 608 (Ch) at paragraphs 85-89. In addition, joint commission of a tort could occur where there is more than mere knowing assistance or facilitation to the degree that the party charged became so involved in the tort as to make it his own; same judgment at paragraphs 103-111. Arnold J held that an injunction was required shutting off access through intermediaries to The Pirate Bay and that same was mandated by European copyright law. That decision, and the others referenced hereafter, make it clear that there is an interest in data protection law terms in internet service providers not only in abiding by their own contract with subscribers but also in avoiding potential liability for, or the grant of an injunction in respect of, copyright infringement.

8.9 The previous year in Twentieth Century Fox Film Corporation & Ors v British Telecommunications plc (Newzbin 2) [2011] 1981EWHC (Ch), Arnold J injuncted the access of BT internet customers to sites called Newzbin 1 and Newzbin 2. These sites were being used to infringe cinema and other copyright. These injunctions required the addition of technology called Cleanfeed onto the computer systems of these firms; though the internet service provider was not required to adopt deep packet inspection based blocking utilising detailed analysis. A similar approach to balancing the proportionality of the order sought judged in the context of the mischief at issue and the competing rights and the burdens and benefits to the parties was taken by Arnold J in Golden Eye (International) Ltd & Ors v Telefónica UK Ltd [2012] EWHC 723 (Ch) in another, but relevant, context. In Australia a different view was taken of authorisation of breach of copyright in terms of the facts both at trial and on appeal to the High Court of Australia in Roadshow Films Pty Ltd v iiNet Ltd [2012] HCA 16.

8.10 To sum up, it is clear that the state of the law was regrettably misconstrued by the Data Protection Commissioner. In that respect, he is not to be faulted as the law is complex. The law does not, however, set intellectual property rights at nought because of the involvement of the internet. In due course, clarity may be brought to the law by a comprehensive ruling where an appropriate case arises before the Court of Justice of the European Union. In the meanwhile, the nature of the injunction sought; the limitation to and the duration of any monitoring; the breadth or narrowness of the scope of any order; the nature of the equipment to be used; the potential for the interference of that equipment with the proper use of the existing systems of the intermediary; the balance of the burden between the parties as to equipment, personnel and cost; the intrusiveness of any remedy into legitimate privacy and the entitlement to communicate; and any potential data protection impingements, together constitute the main factors in a court determining where the proportionality of an injunctive remedy to the mischief of the improper use of intellectual property online is to be struck or whether, on the other hand, an injunction application is to be refused, despite legal compliance, on discretionary grounds.

Criminal conviction
10.0 Beyond a short additional comment, the Court is not required to consider issues as to sensitive personal information in the context of data processing. This has been fully dealt with in the previous decision of this Court. Counsel for the Data Protection Commissioner submitted that an elderly lady receiving a letter from Eircom stating that someone in her household had uploaded a copyright work without authorisation would fear that she was now about to be prosecuted for a criminal offence. The infringement of copyright, if done deliberately with knowledge of the copyright nature of a work copied, can be a criminal offence. There are lots of criminal offences. Many are co-terminus with civil liability. Many actions require analysis to see if a crime has been committed. If a man dies of a heart attack on someone's doorstep and splits his scalp on the door knob in collapsing, the discovery of that body by police is not to be assumed to be murder. If a stone falls from the parapet of the Four Courts building and kills a pedestrian on the pavement below, no criminal offence is necessarily committed even though at the time there was a person on the roof hoisting the national flag. The fall of the stone could be due to the bombardment of the building in the civil war of 1922 and a series of severe winters loosening fragile mortar. If the stone fell due to the negligence of the builders restoring the dome of the Four Courts then if a very serious form of neglect amounting to criminal negligence was proved, a criminal case of manslaughter would arise. If a man pushed a stone onto his enemy below, that deliberate act would be murder if he thereby intended to kill him or cause him serious injury. It would be reckless endangerment if his intention was merely to give him a shock.

10.1 The receipt of a letter by an Eircom subscriber pointing out that someone having access to the internet has downloaded a copyright track or video is not an allegation that the subscriber has committed a criminal offence. The recording companies have no interest in seeking out information from Eircom as to who that subscriber might be. Any serious criminal lawyer considering a prosecution would need to know how many persons might potentially have had access to computers within the house at that particular time of the download or upload. An infringement of copyright could be accidental, could be initiated by an employee, remembering that there is no vicarious responsibility in criminal law, or by a child under the age of responsibility. The particular mental element must be shown to be present by compelling proof: otherwise there is no criminal offence. The Data Protection Commissioner seems to take a clear view that criminal remedies should be kept separated from civil redress for copyright. While that view is commendable, the protocol has nothing to do with accusing anyone of a crime.

Reasons
11.0 Section 10(4)(a) of the Data Protection Acts 1988-2003 provides that: "An enforcement notice shall … specify any provision of this Act that, in the opinion of the Commissioner, has been or is being contravened and the reasons for his having formed that opinion …".

11.1 It follows that counsel for the Data Protection Commissioner was put in an impossible position in being required to argue, as inventively he did, that reasons had been given within the notice of 11 January 2012. The notice contains no reasons whatsoever. There is no warrant from the relevant legislation to overturn a series of decisions of the courts in judicial review whereby reasons are required for administrative actions which settle the entitlements of citizens pursuant to a legislative mandate. In some instances, reasons are simply required by legislation. This is one of those cases. The courts cannot overturn that legislation but are required to implement it. In other cases, an entitlement to reasons may be argued to be a legal right by those whose rights are overturned or gravely affected by an administrative or quasi-judicial decision. Where a licensing authority refuses to grant a permit but fails to give reasons, the applicant for the licence will have no means of knowing what it was she or he did wrong and what it might be that she or he would be required to do correctly in order to be permitted, for example, to open a business legitimately, to operate a fishing trawler or to otherwise pursue permission for an activity that is licensed on meeting specified conditions that are for the benefit of the entire community. Since access to the courts is a constitutionally guaranteed right, an applicant for permission, or a party prevented from an otherwise lawful activity by reason of a decision, is entitled to challenge that decision by judicial review and has an entitlement not to be impeded by the mysterious recitation of reference to legislation of a primary or secondary kind without any real knowledge as to why a decision was taken.

11.2 Sometimes the requirement for reasons can be met in terse terms. A useful test is whether a reasonable person who has heard the entire of the case, or a person who has read all of the relevant papers, would on hearing or reading the decision or judgment be apprised of the reasons for the decision. Regularly, convictions take place in the criminal courts on the basis that a jury accepted the prosecution case and rejected that of the accused, if any. In the District Court, it is perfectly lawful for a judgment to be given in one sentence of a kind which indicates that, for example, in a civil case the evidence of one driver is much more reliable than that of the other because his evidence was more honest, or in a criminal case that the evidence of a particular witness for the defence has made the judge reasonably doubt the prosecution case. In some kinds of administrative procedure, an inspector or other official would do the groundwork before a decision is taken. Planning is an example. A reference in a decision to refusing or accepting the reasons given by such a person clearly mandates the underpinning of the decision with sufficient material to enable judicial review and to inform the citizen. Reasons are not to be judged as inadequate on the terms in which they are put but instead are to be assessed by reference to what a reasonable person with full knowledge of the background would conclude by reading the relevant text.

11.3 The authorities merely amplify the propositions just set out. This Court has no intention of adding to what are clear principles

that are upheld on an invariable basis that is fundamental to the decision making in judicial review. In Sister Mary Christian & Ors v Dublin City Council [2012] IEHC 163, Clarke J at paragraphs 8.15-8.16 summarised the relevant rules in this way:

> 8.15 It must be recalled that the underlying jurisprudence in respect of the obligation to give reasons suggests that the basis for the obligation (in the absence of an express statutory requirement) is to enable the court to exercise its legitimate judicial review function. In at least some cases if a court does not know why a decision was taken, then the court may not be able to ascertain whether the decision was lawful for the lawfulness of the decision in question may depend on whether the reasons were valid in the light of the appropriate statutory and legal regime applicable. The rationale behind the requirement to give reasons was articulated by Kelly J. in Mulholland v. An Bord Pleanála (No. 2) [2006] 1 I.R. 453, at pp. 460 et seq., where, in the section headed "the purpose of reasons" and quoting from earlier case law, he held that:
>
> "In O'Donoghue v. An Bord Pleanála [1991] I.L.R.M. 750 Murphy J. said at p. 757:-
>
> > 'It is clear that the reason furnished by the Board (or any other tribunal) must be sufficient first to enable the courts to review it and secondly to satisfy the persons having recourse to the tribunal that it has directed its mind adequately to the issue before it. It has never been suggested that an administrative body is bound to provide a discursive judgment as a result of its deliberations …'

Likewise, in State (Sweeney) v. Min. for the Environment [1979] I.L.R.M. 35, Finlay P. stated at p. 37 that the purpose of the requirement for reasons was:-

> '… to give … [to an] applicant such information as may be necessary and appropriate for him, firstly, to consider whether he has got a reasonable chance of succeeding in appealing against the decision of the planning authority and secondly to enable him to arm himself for the hearing of such an appeal.'"
>
> 8.16 It is, of course, the case that Kelly J., in Mulholland, was concerned with reasons required to enable a person to consider a statutory appeal within the planning system. However, in Meadows v. Minister for Justice [2010] 2 I.R. 701, at p. 732, Murray C.J. (part of the majority in that case) suggested that the failure of the Minister in question to supply adequate reasons meant that the applicant's "constitutional right of access to the courts to have the legality of an administrative decision judicially reviewed could be rendered either pointless or so circumscribed as to be unacceptably ineffective". While Meadows was, of course, a case in the immigration field, there is no reason why, at the level of principle, the comments of Murray C.J. are not applicable in an appropriate way in respect of any other type of statutory or administrative decision. The underlying rationale of cases such as Meadows (in that respect) and Mulholland is that decisions which affect a person's rights and obligations must be lawfully made. In order to assess whether a relevant decision is lawful, a party considering a challenge, and the court in the event of a challenge being brought, must have access to a sufficient amount of information to enable an assessment as to lawfulness to be made. What that information may be, may vary enormously depending on the facts under consideration or the nature of the decision under challenge. However, the broad and underlying principle is that the court must have access to sufficient information to enable the lawfulness of the relevant measure to be assessed.

11.4 It is clear that the absence of reasons in the Data Protection Commissioner's notice vitiates its validity. Curial deference cannot be pleaded so as to provide a way out of abiding by basic administrative law.

Alleged mis-invocation of jurisdiction

12.0 In seeking judicial review from the High Court there has been no abuse of the remedy of judicial review by the recording companies. An appeal is open to Eircom against the notice of 11 January 2012. No such appeal is automatically open to the recording companies. They were not party to the notice and have no automatic entitlement to make submissions on it. There is no doubt about the entitlement of an interested party to have reasons for a decision which directly affects their economic interest in a substantial way. In Davitt v Minister for Justice (Unreported decision of High Court, Barron J 8 February 1989) and The State (Christopher Philpott) v The Registrar of Titles [1986] ILRM 499 the court found that the failure to notify affected parties of a potential decision was sufficient to render the later decision invalid as a breach of justice.

12.1 It is not impressive that the Data Protection Commissioner, when Eircom appealed that notice pursuant to statute to the Circuit Court, sought to impede the joinder of the recording companies. His reasons were again costs, apparently. The appeal, although lodged, has not been substantively progressed by any of the parties. In the context of an application by the recording companies to be joined, by affidavit dated 31 January 2012, the Data Protection Commissioner swore:

> I say that I am concerned that ... the position is that the applicants wish to make submissions of a generalised nature concerning unlawful filesharing or downloading and/or the extent of the law is caused by such activities and/or the applicant's opinion as to the proper response required by regulatory bodies in order to address these activities. Whilst I fully accept that these are very serious issues in which the applicants have a legitimate interest, they are not issues that are relevant to the determination of the within appeal, not least in circumstances where the within appeal will not involve a reconsideration of the merits of my decision "de novo"… specific reference is made in [an affidavit on behalf of the record companies] two separate proceedings issued by the applicants against the State. I say that if this is the case and if the said companies but wish to make submissions targeted, ultimately, at matters falling outside the scope of the within appeal or so as to influence the future development of the law in this area then that is something that they should do in the appropriate forum at their own expense and not a potential expense of this office ... Clearly if the four record companies are permitted to participate in the appeal it will greatly adds to its length and to the costs that will be incurred by all parties, my office included ...

12.2 During the course of this hearing, no one could definitively say what the scope of the appeal from the Data Protection Commissioner to the Circuit Court was. No one could definitively say what if anything would satisfy the Data Protection Commissioner in his concerns apart from abandoning the protocol in its entirety. Both Eircom and the recording companies have an entitlement to an adjudication by the Data Protection Commissioner in accordance with law. This has not occurred. Judicial review is therefore a proper remedy. As to whether it is appropriate, this Court is bound by the decision in Stefan v Minister for Justice [2001] 4 IR 203 where at 217, speaking for the Supreme Court, Denham J stated:

Once it is determined that an order of certiorari may be granted, the court retains a discretion in all the circumstances of the case as to whether an order of certiorari should issue. In considering all the circumstances, matters including the existence of an alternative

remedy, the conduct of the applicant, the merits of the application, the consequences to the applicant if an order of certiorari is not granted and the degree of fairness of the procedures, should be weighed by the court in determining whether certiorari is the appropriate remedy to attain a just result.

12.3 Similarly, in the earlier decision of McGoldrick v An Bord Pleanála [1997] 1 IR 497 at 509 Barron J stated that:

> The real question to be determined where an appeal lies is the relative merits of an appeal as against granting relief by way of judicial review. It is not just a question whether an alternative remedy exists or whether the applicant has taken steps to pursue such remedy. The true question is which is the more appropriate remedy considered in the context of common sense, the ability to deal with the questions raised and principles of fairness …

12.4 This Court is convinced that in all the circumstances of the case that judicial review was properly and appropriately invoked. The Court has a discretion. The Court exercises that discretion by stating that the choice of judicial review was not misplaced, but was clearly required on the facts, and that legal guidance was properly sought in and from the High Court.

Opposing views
13.0 The regulation of the internet draws forth diametrically opposed views. The use of electronic communication in the democratic revolutions of recent years testifies to the importance of freedom of communication and that this may be undermined by any form of interference in internet communications. Creativity is the engine of the arts industry which brings us new insights and refreshment of the mind in the form of cinema and music. Copyright is no less important than any other intellectual property right. Protection of creativity is central to the law of any sound economic system. Some, as the original complainant in this case, will take a point of view of privacy similar to that ostensibly taken by Advocate General Cruz Villalón in Scarlet Extended; but often quoted out of context. A creative artist desperate for sales of her recorded songs, or an inventor wishing to protect a patent that is the result of years of committed research, may not see the use of the internet as the medium for the breach of their rights as an automatic answer to appropriate legal regulation.

13.1 There is undoubtedly a tension between legitimate expectations of freedom and the entitlement not to have overturned the right to reasonable remuneration for creative endeavor. However, intellectual property rights that have been part of the legal landscape in this jurisdiction since 1710, and that tension can only be resolved by considered political action. Such legislation as currently binds the citizens of this State, and the balance which has so far been struck between copyright and other competing rights, is a matter for administrative and judicial implementation. The duty of the courts is to apply that law in the manner in which it is found. In terms of public administration through quasi-judicial decision-making and the promulgation of appropriate administrative rulings, the task faced is identical and the requirement for legal certainty demands strict compliance.

Result
14.0 In the result, the enforcement notice of 11 January 2012 is invalid in failing to give reasons. Such reasons as appear to underpin it, to the extent that these can be at all ascertained, involve a misconstruction of the relevant law. The enforcement notice is therefore quashed. Such guidance as is appropriate is given in this judgment in the hope of providing some clarification.

14.1 I will hear submissions as to a stay to facilitate any appeal to the Supreme Court, the referral of questions to the Court of Justice of the European Union having been rejected by all parties, and as to costs and as to the possible measurement thereof.