

When Rights Clash Online: The Tracking of P2p Copyright Infringements Vs. the EC Personal Data Directive

OKECHUKWU BENJAMIN VINCENTS*

Introduction

'Anti-piracy Group Broke Swedish Data Laws'. This was the headline to a news story published on the 10th of June 2005 by The Local, a Swedish online news publication. As it turns out, one of Sweden's anti-piracy groups, Antipiratbyrå (APB), in its bid to track copyright infringers, allegedly processed the personal data of Swedish peer to peer (p2p) file sharers in contravention of the Swedish Personal Data Act. This story is representative of the divergent perspectives that have been adopted by copyright owners and p2p file sharers. On one hand, a review of postings in some of the forums frequented by p2p participants indicates that some file sharers assume that there should be a legal rule by which copyright holders are prevented from invading their privacy. On the other hand, developments in the US go to show that the copyright holders seem to have taken the view that the fight against online copyright infringements should supersede all privacy considerations. There is therefore an apparent clash between two well-recognised rights, copyrights and data protection/informational privacy. The need to carefully consider this clash with a view to a possible resolution has now inspired this paper.

* PhD Candidate, National University of Singapore LL.M (International Human Rights Law), Lund University Master of International and Comparative Law, Uppsala University. 39 Prince George's Park Block 13 Unit 6 - 40 Singapore 118431 Singapore Phone: +6598199452 Email: g0600693@nus.edu.sg; ben.vincent@yahoo.com

The paper basically asks if this clash exists and goes ahead to determine the points at which the clash occurs. The Berne Convention, the EC Copyright Directive and the Swedish Copyright Act are the provisions considered regarding the exclusive copyrights violated during p2p file sharing, while the EC Personal Data Directive is considered regarding the privacy rights that are implicated in some of the battle methods of the copyright holders. Two points of clash are identified in the paper. The first is when right holders track online infringements and harvest IP addresses; while the second is when right holders seek to unmask the persons behind the harvested IP addresses. A possible solution to this clash may well be reached if the copyright holders scrupulously observe all the data protection safeguards provided for in the Directive. Although the paper mainly addresses European law, developments in the United States are referred to in order to adequately highlight the clash and the technologies involved.

1 Background

Traditionally, copyright protection is linked to the form of expression of the work. Today however, the content of artistic or literary digital works and other subject matter can be represented in a form independent of any particular medium. This attribute of digital works is commonly referred to as the dematerialisation or de-coupling of works. A sound recording could, for example, be fixed on a compact disc. Depending on the size thereof, it could also be fixed unto a floppy disc. As recent experiences have shown, such a recording may even be inscribed in no singularly identifiable medium. A good example of the latter is the publication by artists of their works on the internet when they were refused publication by recording companies. It is this dematerialisation and the attendant ease of copying, adaptation, and communication of works in digital form that has given rise to the migration of copyrighted works and their exploitation to the internet. The said ease of copying, adaptation and communication has in turn facilitated the Peer-to-peer copyrights infringement phenomenon that forms the crux of this paper.

1.1 *Peer-To-Peer File Sharing*

Peer-to-peer or p2p file sharing is the trading of files in a network of peer nodes. A node is a device such as a computer, a personal digital assistant (PDA) or a cell phone, which is connected as part of a network.¹ 'A pure peer-to-peer network does not have the notion of clients or servers, but

¹ See Wikipedia "Nodes (networking)." http://en.wikipedia.org/wiki/Node_%28networking%29 accessed on 17 February 2006.

only equal *peer* nodes that simultaneously function as both “clients” and “servers” to the other nodes on the network.² P2p networks are the opposites of client-server networks where communication is to and from a central server such as in a File Transfer Protocol (FTP) server. In an FTP server, the client always initiates the download while the server can only respond to requests.³

Connected to p2p networks in the fashion described above, individuals are able to swap different kinds of files including movies, software, music, games and almost any kind of data in digital format. P2p technologies are also employed in other beneficial services like in facilitating telephony traffic. The benefits notwithstanding, the technologies have been a source of controversy in recent years primarily because the preponderance of files shared in such networks are copyright protected and are hitherto shared with no restraints and still with no compensation whatsoever to the copyright owners.

1.1.2 *First Generation P2p Applications*

P2p file sharing technologies have developed in three distinct generations. The first generation saw its demise in the US case of *A&M Records Inc. v. Napster* (2001).⁴ Discoveries in that case indicate that Napster developed and distributed a type of software known as MusicShare. This software operated a p2p protocol that made MP3 music files stored on individual computer hard drives available for copying by other Napster users; it facilitated the search for such files; and enabled the transfer of exact copies of MP3 files from one computer to another via the Internet. However the development and distribution of this and similar software came to an end after the court ruled that Napster was contributorily and vicariously liable for the copyright infringements of the end users of its software. The 2nd and 3rd generations of p2p file sharing applications are however still very much in use.

1.1.3 *Second Generation P2p Applications*

Discovery in the US case of *Metro-Goldwyn-Mayer Studios Inc V. Grokster, Ltd*⁵ reveal the working of two types of the 2nd generation p2p applications namely, Grokster, which runs on the ‘FastTrack’ technology; and Morpheus, which runs a similar technology known as the ‘Gnutella’ technology.

² Wikipedia “Peer-to-peer” <http://en.wikipedia.org/wiki/P2p> accessed on 17 February 2006.

³ See generally, Wikipedia, *Supra* note 1.

⁴ 239 F.3d 1004, 2001 Copr.L.Dec. P 28,200, 57 U.S.P.Q.2d 1729, 01 Cal. Daily Op. Serv. 1255, 2001 Daily Journal D.A.R. 1611 (Westlaw).

⁵ 545 U.S. 913 (Westlaw International).

Grokster was distributed by Grokster Ltd, while Morpheus was distributed by StreamCast Networks Inc. According to Justice Souter:

Grokster's eponymous software employs what is known as FastTrack technology, a protocol developed by others and licensed to Grokster. StreamCast distributes a very similar product except that its software, called Morpheus, relies on what is known as Gnutella technology. A user who downloads and installs either software possesses the protocol to send requests for files directly to the computers of others using software compatible with FastTrack or Gnutella. On the FastTrack network opened by the Grokster software, the user's request goes to a computer given an indexing capacity by the software and designated a supernode, or to some other computer with comparable power and capacity to collect temporary indexes of the files available on the computers of users connected to it. The supernode (or indexing computer) searches its own index and may communicate the search request to other supernodes. If the file is found, the supernode discloses its location to the computer requesting it, and the requesting user can download the file directly from the computer located. The copied file is placed in a designated sharing folder on the requesting user's computer, where it is available for other users to download in turn, along with any other file in that folder.⁶

The typical 2nd generation p2p application or software thus requires the user to designate a directory or directories in his hard drive as part of the p2p network. In other words, the designated directories are marked as 'shared'. The contents of the designated directories are automatically broadcast or made available for downloading throughout the network whenever the user connects. In effect, whenever the user logs unto the network to download files, he or she is at the same time uploading files. If the files in the designated folders and the ones being downloaded unto those same folders are copyright protected, the user would not only be illegitimately making copies but also unlawfully communicating the protected works to the public by a single act.

1.1.4 *Third Generation P2p Applications: Bit Torrent*

BitTorrent is the name of the third generation p2p file distribution protocol, and is also the name of one of the free software that implements that protocol. The protocol was originally designed and created by programmer Bram Cohen, and is now maintained by BitTorrent Inc. BitTorrent is designed to widely distribute large amounts of data without incurring corresponding consumption in costly server and bandwidth resources.

⁶ *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, LTD* 545 U.S. 913 (Westlaw International).

The end user application that runs the Bittorrent protocol is known as the Bittorrent Client and examples include: BitTorrent, distributed by Bram Cohen's BitTorrent Inc; Azureus, distributed by SourceForge.net; and BitTornado. These applications are employed in the creation, download and upload of torrent files, which in turn may contain copyright protected files. According to Bram Cohen,

To start a BitTorrent deployment, a static file with the extension .torrent is put on an ordinary web server. The .torrent contains information about the file, its length, name, and hashing information, and the url of a tracker. Trackers are responsible for helping downloaders find each other. They speak a very simple protocol layered on top of HTTP in which a downloader sends information about what file it's downloading, what port it's listening on, and similar information, and the tracker responds with a list of contact information for peers which are downloading the same file. Downloaders then use this information to connect to each other. To make a file available, a 'downloader' which happens to have the complete file already, known as a seed, must be started. The bandwidth requirements of the tracker and web server are very low, while the seed must send out at least one complete copy of the original file.⁷

Although the bittorrent is different in architecture from the 2nd generation protocol, they both share a significant similarity in that, like in the 2nd generation platform, a bittorrent downloader could also be uploading or communicating protected files in the same act. In other words, a file sharer in the bittorrent platform could be seeding and downloading seeded files at the same time.

1.1.5 *P2p Circumventions*

BitTorrent networks are even designed to counteract and circumvent most anti-piracy measures instituted by groups representing copyright owners. In the wake of the legal proceedings that shut down Napster, the second generation networks like Kazaa obviated with reliance on central servers and relied on decentralised indexing servers known as 'Supernodes' and circumvented 'spoofing'. Spoofing is one of the anti-piracy measures employed by copyright owners and it involves the flooding of p2p networks with decoy or spoofed files made up of unusable content.⁸

⁷ Bram Cohen 'Incentives Build Robustness in Bit Torrent' (May 22 2003) <http://www.bittorrent.org/bittorrentecon.pdf> accessed on 30 October 2006.

⁸ See generally Bay TSP Corporation 'Whitepaper: Combating Online Software Piracy in an Era of Peer-to-Peer File Sharing' (2004) available online at <http://www.baytsp.com/downloads/WhitePaperFinal.pdf> accessed on 17 February 2006.

The bittorrent networks, mentioned above, took the technology further by introducing advanced ‘swarming’ technologies and have tried several methods of hiding the identity of the end users behind the nodes. This was done through *inter alia* the use of encrypted downloading technologies, which have not been totally successful. Swarming allows downloaders to obtain pieces of a file from different nodes simultaneously.⁹ In sum, it is obvious that p2p file sharing networks are supported by very advanced technologies that have proven quite efficient in operation.

1.2 *The Battle Methods of the Right Holders*

Organised in collective rights protection groups such as the International Federation of Phonogram and Videogram Producers (IFPI), Recording Industry Association of America (RIAA), Antipiratbyrå (APB), Sweden, copyright owners have adopted a number of strategies to combat p2p infringements. For our purposes, the most significant of these strategies consists of online tracking and subsequent enforcement. To track online infringements, the groups scour the internet for persons sharing protected files. This they do by the use of applications known as ‘bots’ or search robots, also known by other names such as ‘spiders’, web crawlers and web robots.

These applications are generally ‘Programs that recursively query other computers over the Internet in order to obtain a significant amount of information...’¹⁰ The right-holder groups, through this type of technologies, gather information on file sharers such as, IP addresses and usernames. All such information is then incorporated into a database. To monitor compliance, the groups also have the ability to establish ‘case files’ in order to track suspected infringers on a long term basis. This is done in order to ensure that they don’t continue to share copyrighted files.¹¹ The fact that right-holder groups employ this method is not in issue since they have never seen cause to deny the use of tracking technologies. Indeed According to RIAA’s website, it’s team of Internet specialists, ‘with the assistance of a 24-hour automated webcrawler, helps to stop Internet sites that make illegal recordings available’.¹²

In the US, based on the Digital Millennium Copyright Act’s (DMCA) expedited subpoena provision, the RIAA for example, as part of an effort to track, shut down, deter, and prosecute offenders, sends out information

⁹ *Ibid.*

¹⁰ *Ebay, Inc. V. Bidder’s Edge, Inc.* 100 F.Supp.2d 1058 at p.1061.

¹¹ See Bay TSP Corporation *Supra* note 8.

¹² Recording Industry Association of America ‘What the RIAA is Doing About Piracy’ <http://www.riaa.com/issues/piracy/riaa.asp> accessed on 28 February 2006.

subpoenas to ISPs in order to identify the persons behind the IP addresses. In Sweden, the information gathered through the search robots are released to the police for further investigation and prosecution. In some countries therefore, information gathered through search robots is presented to ISPs with a demand for the 'real life' information of the persons using the IP addresses, while in others a report is made to the police for further action.

1.3 *The Personal Data/Privacy Questions*

Two broad privacy questions are raised by the battle methods presented above. The first is on the use of search robots and it basically asks whether the harvesting of Internet Protocol addresses and any other personal information amounts to processing of personal data. The second centres on the aftermath of the online tracking and harvesting of IP addresses and basically asks if, when, and how internet service providers should release the private information of their clients to right holders. Complaints on the battle methods of the right holders in Sweden have addressed mainly the first question while the legal battles that right holders have had to face in the United States in prosecuting offenders have touched mainly the second question. According to a Swedish local news report, thousands of Swedes had in March 2005 reported APB, the film and games industry-backed organisation, to the Swedish Data Inspection Board for its method of tracking the downloading of copyright-protected files. The Data Inspection Board then ruled that if an IP address can be linked to an individual it is classed as personal information and therefore falls under the Personal Data Act, the Swedish implementation of the EC Personal Data Directive.¹³ This news was however followed by another that reported The Swedish Board of Data Inspection as deciding that organisations such as IFPI have the right to gather and store IP addresses identifying every computer on the internet.¹⁴ In the US, complaints from an ISP that was subpoenaed for 'real life' information of one of its clients gave rise to the case of *RIAA v. Verison Internet Services*.¹⁵ Verison, an internet service provider, refused to honour RIAA's subpoena, which is supposedly based on the US Digital Millennium Copyright Act, because it believed that such a subpoena, without a court order will unwarrantedly violate the constitutional right to privacy of its clients.¹⁶

¹³ The Local 'Anti-Piracy Group broke Swedish Data Laws' 10 June 2005 <http://www.thelocal.se/article.php?ID=1581> last visited on 25th July 2005.

¹⁴ The Local 'Swedes Face Massive Fines for Sharing Songs Online' 15 November 2005 <http://www.thelocal.se/article.php?ID=2496> visited on 18 November 2005.

¹⁵ Suit No 03-7015 United States Court of Appeal, District of Columbia Circuit.

¹⁶ Jonathan Krim 'A Story of Piracy and Privacy' Washington Post 5 September 2002 <http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A38034-2002Sep4> visited on 10 January 2006.

The Article 29 Working Party¹⁷ has voiced concerns similar to those revealed by the privacy questions under consideration. In its 2005 ‘Working Document on Data Protection Issues Related to Intellectual Property Rights’ (WP104), The working party considered the identification and tracking of individuals accessing protected files and the subsequent enforcement by right holders. It then observed that ‘...some of these measures aimed at ensuring the effective protection of some copyright material against alleged unlawful exchange, taken at various levels by copyright holders, involve the processing of personal data of individuals.’¹⁸ It also concluded the working document by stating that ‘As far as the investigation powers is concerned, the Working Party deems it necessary to recall that investigations performed by private actors such as copyright holders must be performed in a clear legal framework.’¹⁹

2 The Clashing Rights/Applicable Laws

So far this paper has thrown some light on the architecture of the p2p file sharing networks and outlined the methods employed by the right holders in fighting online infringements. The personal data questions have also been adumbrated. The following parts of the paper will seek to substantiate the existence of the clash between the protection of copyright and the protection of personal data. The first step towards discharging this task will be to provide an outline of the substantive laws implicated in the apparent clash. Thereafter, analysis will be geared towards a possible resolution. The fact that right holders have the right to end the infringement of their copyrights is beyond question. It is also beyond question that the existence of copyright does not extinguish the privacy protection conferred by data protection laws. It remains then for the present discourse to locate the appropriate point of balance.

2.1 *The Specific Copyrights Infringed in P2p File-Sharing*

2.1.1 *Reproduction Rights*

The typical p2p application requires the user to designate directories in his hard drive as part of the p2p network and the contents of the designated directories are automatically made available for downloading throughout the network whenever the user signs in. In effect, whenever the user signs

¹⁷ An independent European advisory body on data protection and privacy, and which was set up pursuant to Directive 95/46/EC (the Personal Data Directive).

¹⁸ Article 29 Working Party ‘Working Document on Data Protection Issues Related to Intellectual Property Rights (WP104)’ 18 January 2005 p.2.

¹⁹ *Ibid.*

into the network to download files, he or she is at the same time uploading files. The right of copyright owners to prevent others from making copies of their works without authorisation is the most basic right under copyright law and other rights in the copyright system like the right to authorise distribution are provided to give teeth to this exclusive right. The exclusive rights to authorise reproduction and communication of works are part of the economic rights of the owners and without them, the right owners may derive no financial reward from the use of their works.

The right of reproduction is infringed when copies are made for placing in the designated directories for others to download and further by the act of downloading by other peers in the network. *Article 9* of the Berne Convention provides that 'Authors of literary and artistic works protected under this Convention shall enjoy exclusive right of authorising the reproduction of these works, in any manner or form.'²⁰ Were states parties to retain the language of the above provision, certain acts of copying involved in p2p file sharing may have fallen outside the ambit of prohibited acts. However, modern copyright enactments are now drafted in terms comprehensive enough to catch all the acts of copying involved in the p2p system. The EC Copyright Directive, for example, provides in Article 2 that 'Member states shall provide for the exclusive right to authorize or prohibit direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part: (a) for authors of their work; for performers, of fixations of their performances; for phonogram producers, of their phonograms; for the producers of the first fixations of films, in respect of the original and copies of their films; for broadcasting organisations, of fixations of their broadcasts, whether those broadcasts are transmitted by wire or over the air, including by cable or satellite.'²¹

Whereas a file sharer under the terms of the Berne Convention may have argued that placing a copyrighted file in a folder in his computer does not amount to copying or that downloading an altered version of a similar work from a peer does not require prior authorization. Such an argument would no longer be tenable within the EU in the light of the terms of the Copyright Directive. The terms 'direct or indirect'; 'temporary or permanent' reproduction as well as 'by any means and in any form' in Article 2 are designed to exclude all such argumentation. In Sweden for example, since the coming into force on the 1st July 2005 of the Copyright Act,²² which implements the EC Copyright Directive, it is fairly understood that p2p file sharing amounts to copyrights infringement when the shared files are protected.

²⁰ Berne Convention for the Protection of Literary and Artistic Works, Paris Act of July 24, 1971 as amended on September 28, 1979.

²¹ Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001, Article 2.

²² Act on Copyright in Literary and Artistic Works (Act 1960:729, of December 30 1960, as Amended up to July 1, 2005) (Swedish Copyright Act).

2.1.2 *Communication Rights*

P2p file sharing of copyrighted works infringes the right of communication to the public when files are uploaded and disseminated through the p2p networks. In Article 11*bis* (1), the Berne Convention also provides that

Authors of literary and artistic works shall enjoy the exclusive right of authorizing: (i) the broadcasting of their works or the communication thereof to the public by any other means of wireless diffusion of signs, sounds or images; (ii) any communication to the public by wire or by rebroadcasting of the broadcast of the work, when this communication is made by an organization other than the original one; (iii) the public communication by loudspeaker or any other analogous instrument transmitting, by signs, sounds or images, the broadcast of the work.²³

Just like the exclusive right of reproduction, the exclusive right of broadcasting and communication to the public as contained in above provision has had to be updated first by the WIPO Copyright Treaty (WCT)²⁴ to include ‘...any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access these works from a place and at a time individually chosen by them.’²⁵ The terms ‘wire or wireless means’ and ‘public access from a place and a time chosen by them’ could be said to cover internet distribution generally and p2p file sharing in particular. Article 3 (1) of The EC Electronic Copyright Directive is enacted in exact terms as Article 8 of the WCT and has been in turn incorporated into the laws of EC member states including Sweden.²⁶ There remains no doubt that p2p file sharing infringes the exclusive rights of reproduction and communication of works and other subject matter within the EU. The same is true of most of the member states of the Berne and Rome²⁷ Conventions as updated by WIPO Copyright Treaty 1996 and WIPO Performances and Phonograms Treaty 1996.

2.1.3 *Exceptions*

As regards Exceptions and limitations to the foregoing rights, suffice it to say that the reproduction and communication carried out in the p2p file sharing systems do not correspond to any of the exceptions and limitations recommended under the Berne Convention neither do they correspond to any of those provided for under the EC Copyright Directive. File

²³ Berne Convention, *Supra* note 20, Article 11*bis*.

²⁴ WIPO Copyright Treaty (WCT) 1996.

²⁵ *Ibid*, Article 8.

²⁶ See Swedish Copyright Act, *Supra* note 22, Article 2.

²⁷ 1961.

sharers interviewed as part of the research of this paper argued that they make only private copies. Under the Directive, the limitation to the exclusive right of reproduction addressed to natural persons who make private copies of works is conditioned upon the payment of fair compensation to the right holders²⁸ and no p2p network has been known to require fair compensation to right holders.

2.1.4 *Distortions, Mutilations and Moral Rights*

In its Article Art 6bis (1), the Berne Convention provides that authors shall independently of their economic rights have the right to claim authorship of the work and the right to object to 'any distortion, mutilation or other modification of, or other derogatory action in relation to, the said work, which would be prejudicial to his honour or reputation.'²⁹ Article 3 of the Swedish Copyright Act is an example of the implementation of Article 6bis. It provides that 'When copies are made of a work, or when it is made available to the public, the name of the author shall be stated to the extent and in the manner required by proper usage. A work may not be changed in a manner which is prejudicial to the author's literary or artistic reputation or to his individuality, nor may it be made available to the public in a form or in such a context as is prejudicial in the manner stated.'

To make peer to peer file sharing possible, peers have to subject music and movie works to ripping, conversion, alterations and modifications of all sorts. Movies are generally published today in DVD (Digital Versatile Disc) and VHS (Video Home System) formats. To share these movies, the peers usually rip the data constituting the movies from the DVD and convert the files from the MPEG-2 (Moving Picture Experts Group-2), which is the coding format for most commercial DVDs, to other more portable formats like DivX (a compression video codec created by DivX inc), AVI (Audio Video Interleave) and many other file formats. Sound recordings are similarly ripped from CDs and converted from Audio CD format to MP3 (MPEG-1 audio layer 3) format. These are all then freely shared on the internet.

While these conversions, coding and trans-coding may not meet with the classical definition of adaptation and translation in copyright law, they however do amount to significant modification and distortion of works and at the very least, would attract the objection envisaged by Art 6bis of the Berne Convention. Such modifications are indeed prejudicial to the reputation of the right holders as envisaged by the Swedish Copyright Act, not only because the coding, ripping and trans-coding lead to sometimes noticeable loss in quality of the subject matter but also because other forms of moral rights are violated.

²⁸ See EC Copyright Directive *Supra* note 21, Article 5 (2) (b).

²⁹ *Ibid*, Article 6bis (1).

2.1.5 *Moral Rights*

The most basic recognition of the moral right of a copyright owner is the indication of the names of the owner or other forms of acknowledgement of the right owner on the works or other subject matter. In a standard DVD movie, this right is satisfied in several ways, on the labels and the prints on the disc, in the recording as in the acknowledgements that are recorded to be played in the beginning and the ending of the movie, and also by the Digital Rights Management (DRM) codes that might be embedded in the disc. Audio recordings satisfy the moral rights through the labels and the DRMs. Even when these works are legally distributed online, efforts are made to at least display minimum information on the authorship of the work.

P2p file sharers on the other hand do not usually give a care about the niceties of moral rights. DRMs are usually removed and there are no accompanying labels to display information on the authorship of the works and, many times, movie files are edited for size reduction. The result of the editing is that the authorship acknowledgements that should play at the end of the movie are sometimes cut off and the cuttings sometimes extend to authorship displays at the beginning of the movies. In more extreme cases, the file ripper embeds his/her own information in the movie file that amounts to claiming authorship. Other forms of mutilation have also been witnessed, this author has seen one such file where the movie starts with a video clip, perhaps of the ripper, shouting 'you f@#&ers'.

Evidently, practices that infringe the moral rights of copyright owners as protected under provisions such as Article 6 of the Berne Convention and Article 7 of the EC Copyright Directive are rife in the p2p file sharing world. The foregoing paragraphs also demonstrate just how deeply the p2p practices go to the very core of copyright protection, infringing the most important of the exclusive rights. Little wonder then that right-holder groups have embarked on a vigorous battle to preserve their rights.

2.2 *Protection of Personal Data: EC Personal Data Directive*

Article 1 of the directive leaves little room for doubt that one of its two objectives is the preservation of the right to privacy. It provides, 'In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. 2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.'³⁰ At this juncture, it is necessary to emphasise some of the

³⁰ Directive 95/46/EC of the European Parliament and of the Council 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, Article 1.

definitions found in Article 2 particularly Articles 2 (a) and (b), ‘personal data’ and ‘processing of personal data’.

For the purposes of this Directive: (a) ‘personal data’ shall mean any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity; (b) ‘processing of personal data’ (‘processing’) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;...³¹

The inquiry into whether or not the information which right holders gather by web crawling amounts to personal data will be considered hereinafter. However, at some point personal data will have to be used by the said right holders and from Article 2(b) above, such ‘use’ and the ‘collection’ as well as the ‘disclosure’ of such information among other activities invariably amount to the processing of personal data.

Article 3 of the Directive delimits its scope, intimating that its provisions apply to the processing of personal data wholly or partly by automatic means as well as to non automatic means that form part of a filing system or are intended to form part of a filing system. Article 3 (2) specifies processing of personal data that falls outside the scope of the directive. These are specifically processing relating to ‘...public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.’ Noticeably the activities of collective right-holder groups are not exempted under Article 3. However in member states where copyright infringement is already a crime, the processing of personal data by state agencies such as the police would fall outside the scope of the Directive.

Having established what amounts to personal data, the processing thereof, and the processing not prohibited by the directive; the next relevant consideration is the criteria for legitimate processing of personal data. Article 7 covers this and provides that

Member States shall provide that personal data may be processed only if: (a) the data subject has unambiguously given his consent; or (b) processing is necessary for the performance of a contract to which the

³¹ *Ibid*, Article 2.

data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or (d) processing is necessary in order to protect the vital interests of the data subject; or (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).³²

From the above provision, if it is established that the information retrieved by copyright holders through search robots amounts to personal information, 7 (a) will apply. Seeing that the data subjects are not aware of the gathering of such information and so could not have given their consent, the only provision under which right holders can legitimize their activities will be Article 7 (f). The question under 7 (f) is whether the fight against p2p copyright infringements amounts to legitimate interests of the right holders. If it does, the next question would be whether or not the right to privacy of the data subjects overrides those legitimate interests. All these are fully considered below.

3 The Clash During Online Tracking

Search robots are part of the internet surveillance technologies that have been causing some disquiet since the well-publicised cases and investigations from 2000 involving some major US companies. Those cases considered the privacy implications of the use of cookies and similar technologies. Nevertheless, the few litigations that were initiated against the use of search robots, notably in the United States, did not meet with overwhelming success in that none of the courts found it fit to outlaw the use of such applications *per se*.

3.1 *Developments in the United States*

In the first of these cases, *eBay v. Bidders Edge*,³³ the defendant, Bidder's Edge (BE), which operated an auction aggregation site, used search robots to access eBay's Web site about 100,000 times per day, accounting for over 1 percent of the internet information requests received by eBay.

³² *Ibid*, Article 7.

³³ 100 F.Supp.2d 1058.

The plaintiff, eBay claimed that it was entitled to injunctive relief because of BE's unauthorized presence. The district court rejected eBay's claim stating that neither such unauthorised presence alone, nor the incremental cost the defendant had imposed on the operation of the eBay site could entitle eBay to injunctive relief. The court however found sufficient proof of threatened harm in the potential for others to imitate the defendant's activity.

In *Intel Corporation v. Kourosh Kenneth Hamidi*,³⁴ the Supreme Court of California rightly pointed out that 'The two district courts, *eBay v. Bidders Edge, Inc.* and *Register.com, Inc. v. Verio, Inc.*,³⁵ that found such automated data collection to constitute a trespass relied, in part, on the deleterious impact this activity could have, especially if replicated by other searchers, on the functioning of a Web site's computer equipment.' In effect, the courts that have had to consider the legality of search robots did not consider them to constitute trespass in principle but found for the plaintiff in the eBay case based on the harm that such web crawling could cause if imitated by others.

The outcome of these cases notwithstanding, a consideration of the effect of web crawling under the tort of trespass is quite different from considering the same issue from the perspective of informational privacy or the processing of personal data of internet users. Within the EU, such surreptitious gathering of information on natural persons would raise issues under the EC Personal Data Directive and under Article 8 of the European Convention on Human Rights,³⁶ which the Directive implements. In every other jurisdiction where the International Covenant on Civil and Political Rights³⁷ is applicable, a similar set of facts would also raise privacy questions. We are however concerned with the EC Personal Data Directive.

3.2 *Online Tracking and Directive 95/46/EC*

As noted above, the crux of a discussion, such as ours, relating to the processing of personal data under the Directive is to determine whether or not such processing is legitimate since the aim of the law in this area is not to prohibit data processing. To be legitimate, the controller of such data must base his/ her activity under one of the paragraphs of Article 7. As regards online tracking by right holders, it is not in dispute that the search robots employed by the right holders do indeed harvest IP addresses. Such harvesting definitely answers to the definition of 'processing' as they amount to 'collecting' such data. Similarly, communicating

³⁴ 30 Cal.4th 1342 at 1354.

³⁵ (S.D.N.Y. 2000) 126 F.Supp.2d 238, 248-251.

³⁶ 1950.

³⁷ 1966.

the same data to law enforcement agencies or any other third party will amount to disclosure by transmission or dissemination.

3.2.1 *IP Addresses as Personal Data*

To proceed, it must be considered whether or not IP addresses are personal data as envisaged by the Directive. It is to be recalled that according to the Directive, personal data is any information that relates to an identified or identifiable natural person and an identifiable person is one who can be identified, *directly or indirectly*, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. To perfunctorily surmise that an IP address is an identification number that can *indirectly* identify a natural person would not seem to be an undue stretching of the language of the Directive. However, a proper analysis of the question calls for a little more than a quick surmising.

An IP address is a 4 to 12 digit number assigned by an ISP to an account holder's computer or other PDA that is connected to the internet (e.g. 193.728.16.44). The fact that the ISP always knows an account holder's 'real world' identity from the IP address allocated to him seems to support the notion that an IP address is personally identifying information. The Article 29 Working Party has unequivocally opined that IP addresses are personal data. In their words: 'The Working Party wishes to emphasise that IP addresses attributed to Internet users are personal data and are protected by EU Directives 95/46 and 97/66.'³⁸

A distinction has however been drawn between 'dynamic' and 'static' IP addresses. Dynamic IP addresses are used where an account holder is allocated a new IP address each time he makes a connection while a static IP address refers to one that is more permanently allocated to an account holder's device like in some broadband and ADSL connections. The transient nature of dynamic IP addresses makes them less likely to qualify as personal data in the hands of persons other than the ISP. At the same time, it is worth noting that static IP addresses would not always be personally identifying since there are situations where even an ISP is not able to identify all the users behind an IP address. The most common example of this situation is where one or more subscribers use a wireless router to share their connection with many other persons.³⁹ In such circumstances, particularly when a wireless network is unencrypted, it would seem unreasonable to consider an IP address as personally identifying vis a vis the unknown users.

³⁸ Opinion 2/2002 of the Working party of 30 May 2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6, WP 58, 10750/02/EN, p 3.

³⁹ See generally M. Watts and M. Jelf 'United Kingdom: Privacy V. Piracy' (Mondaq-Legal Practitioners, 7 September 2005) available online at http://www.mondaq.com/i_article.asp_Q_articleid_E_35006 last visited 24 March 2006.

Is it then safe to conclude that IP addresses are personally identifying as regards, at the very least, the subscribers whose 'real world' identities are known by their ISP? It is the opinion of this author that the European Court of Justice (ECJ) is likely to answer in the affirmative. The Personal Data Directive has a very broad scope and in its first case on which it was called upon to interpret the Directive, the ECJ subscribed to this broad scope. *Case C-101/01* was a reference to the court under Article 234 EC by the Göta hovrätt, Sweden for a preliminary ruling in the criminal proceedings before that court against Bodil Lindqvist.

Mrs Lindqvist had set up internet pages at home on her personal computer in order to allow parishioners, in the parish of Alseda, Sweden, preparing for their confirmation to obtain information they might need. A link was also set up between those pages and the website of the Swedish Church. The said pages contained information about Mrs Lindqvist and 18 colleagues in the parish including names, family circumstances, telephone numbers and other matters. Mrs Lindqvist had neither informed her colleagues of the existence of those pages nor obtained their consent. She also did not notify the Datainspektionen (supervisory authority for the protection of electronically transmitted data) of her activity. One of the questions referred to the ECJ was '...whether the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes the processing of personal data wholly or partly by automatic means within the meaning of Article 3(1) of Directive 95/46.'⁴⁰

The Court answered the above question in the affirmative, stating that the term personal data as used in Article 3(1) of Directive 95/46 covers any information relating to an identified or identifiable natural person. The Court further reasoned that the term undoubtedly covers the name of a person in conjunction with his telephone coordinates or information about his working conditions or hobbies. The ECJ has in effect held that the term 'personal data' includes any of the following relating to an identified or identifiable natural person: his name in conjunction with his telephone coordinates; his name in conjunction with information on his working conditions; his name in conjunction with his hobbies. Unfortunately, the facts of the *Bodil Lindqvist case* do not lead to an analysis that throws much light on the consideration of IP addresses as personal data. However the court's decision, particularly on what constituted personal data in that case, reveals a willingness to go along with the broad scope of the Directive. This is more so since it went ahead to reach an overall decision that did not in any way detract from the said broad scope. The ECJ

⁴⁰ Judgment of the Court of 6 November 2003 in Case C-101/01 (Reference for a preliminary ruling from the Gota hovrätt): Bodil Lindqvist.

is therefore very likely to take a broad view that would treat IP addresses as personal data at least in some circumstances. Such a decision is most likely going to turn on the meaning the court would choose to assign to the clause ‘information relating to an identified or identifiable natural person’ in Article 3 (1). While the file sharers may not be regarded as identified persons in most cases where their IP addresses are harvested. It is however safe to conclude that the file sharers are always *identifiable* through their IP addresses and as such the IP addresses constitute information relating to identifiable natural persons.

3.2.2 *The Legitimacy of Harvesting IP Addresses*

From the wordings of Article 7(a), Member States shall provide that personal data may be processed only if the data subject has unambiguously given his consent. This provision practically amounts to a prohibition of surreptitious processing of personal data such as the online tracking performed by right holders over infringing p2p file sharers. Paragraphs (b) to (f) of Article 7 could be viewed as exceptions to the general rule in 7 (a) that the data subject must unambiguously give his consent before his data could be processed. Copyright owners would therefore find it difficult to legally justify the use of search robots to gather the type of information they currently gather except under paragraph (f).

By Article 7 (f), member states are to provide that personal data may only be processed if ‘processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).’ This provision raises two important questions. Firstly, does the protection of the copyright to their works amount to the legitimate interests of the right holders? Secondly, does the fundamental right to privacy of the file sharers in any way override the legitimate interests of the copyright holders? This paragraph probably summarises the question of this paper i.e. the apparent conflict between copyrights and the right to privacy.

3.2.3 *The Legitimate Interests of Copyright Holders*

The term ‘legitimate interest’ is one of those terms that, although pervasive in EC legislation, have not been assigned any specific meaning in any of the many instruments in which they appear. Naturally, the term is therefore to be assigned its ordinary meaning. The Cambridge Advanced Learners Dictionary (CALD) assigns two meanings to the word ‘legitimate’. The first is ‘allowed by law’ while the second is ‘reasonable and acceptable’ it is submitted that both meanings are envisaged in the use

of the term in Article 7 (f).⁴¹ CALD also defines ‘interest (legal right)’ as ‘an involvement or a legal right, usually relating to a business or possessions’.⁴² The nature and extent of copyright violations in p2p file sharing, amply demonstrates that copyright holders do indeed pursue legitimate interests in seeking to track p2p file sharers. Any processing of personal data that result in these pursuits should therefore be deemed legitimate except that the right holders still have to show that the right to privacy of the file sharers does not override their legitimate interests.

3.2.4 *Overriding Interests of Fundamental Rights and Freedoms of Data Subjects*

Contemporary views on human rights as outlined in international instruments are that they are to be accorded overarching implementation. This view stems from a firm understanding that these rights are meant, just as acknowledged by Article 7(f), to be indeed overriding. A careful consideration of the major human rights treaties reveals that the corollary of this overriding status is that exceptions to the rights or derogations from them are only permissible in very narrowly defined circumstances.

Regarding the particular right to privacy referred to in Article 1 (1) of the Directive, an example of the narrow circumstances under which the right would cease to be overriding is found in Article 8 (2) of the ECHR. Considering this provision specifically in the light of the legitimate interests of copyright holders, the right to privacy would not be overriding only under situations or procedures that are in accordance with the law and which are necessary in a democratic society in the interest of the economic well being of the country, for the prevention of crime or for the protection of the rights of others.

Economic well being of the country, the prevention of crime and the protection of the rights of others respectively could therefore necessitate interference with the right to privacy within clear legal boundaries. Adequate protection of intellectual property rights is relevant to the economic well being of a country since successful participation in the global market is increasingly linked to strong protection of intellectual property rights including copyright and neighbouring rights. The prevention of crime acquires heightened relevance in countries where copyright infringements, such as the ones that go on in p2p file sharing, have been outlawed as criminal wrongs. Even regarding those countries where such infringements are yet to become crimes, calls for criminalisation continue to be heard.

⁴¹ Cambridge Dictionaries Online ‘Legitimate’ <http://dictionary.cambridge.org/define.asp?key=45473&dict=CALD>.

⁴² *Ibid* ‘Interest’ <http://dictionary.cambridge.org/define.asp?key=41422&dict=CALD>.

As regards the rights of others, intellectual property rights including copyright and related rights are regarded as third generation human rights and are duly recognised as human rights under Article 27 (2) of the Universal Declaration of Human Rights⁴³. The Article provides that ‘Everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author.’

In sum, there is little doubt that the ECJ is likely to hold that the protection of their copyrights from infringements of the p2p magnitude amounts to legitimate interests of the right holders that necessitates and consequently makes the processing of personal data permissible within clearly defined legal limits. These legal limits may well be partly seen in the Directive’s provisions on the principles relating to data quality and other national provisions that prescribe due process as will be considered below.

4 The Clash During Offline Copyright Enforcement

4.1 *Copyright Enforcement*

Copyright enforcement is to be understood in this paper to refer to the various processes embarked upon by right holders after the tracking phase of their battle against p2p file sharers. These processes generally include further investigation to unmask the users of identified IP addresses by obtaining their detailed information from their ISPs; the serving of ‘cease and desist’ notices; and the judicial prosecution of identified offenders. The enforcement paths used and the successes thereof have varied considerably depending on the country in question. In Belgium, right holders seek the collaboration of ISPs, who themselves serve ‘cease and desist’ notices to the offending subscribers; in Sweden, the matter is generally reported to the police for further action while in the United States, right holders have hitherto served subpoenas on ISPs to release detailed information of the users behind the infringing IP addresses.

4.2 *Developments in the United States*

The United States Court of Appeal case, *Recording Industry Association of America, Inc., (RIAA) v. Verizon Internet Services, Inc.*⁴⁴ has heralded the call for due process in copyright enforcement related to p2p file sharing. The

⁴³ 1948.

⁴⁴ 351 F.3d 1229, 359 U.S.App.D.C. 85, 2004 Copr.L.Dec. P 28,734, 69 U.S.P.Q.2d 1075, 31 Communications Reg. (P&F) 438.

facts of the case reveal that RIAA served two subpoenas on Verizon, an internet service provider. The subpoenas were meant to compel Verizon to disclose the names of two of its subscribers who appeared to be trading large numbers of .mp3 files of copyrighted music via p2p networks. Verizon refused to comply with the subpoenas on various legal grounds. The matter went to trial and the district court rejected Verizon's statutory and constitutional challenges to § 512(h) DMCA and ordered it to disclose to the RIAA the names of the two subscribers. After Verizon failed to quash a second subpoena, it appealed the two district court orders to disclose. Consolidating the cases, the Court of Appeals held that under the Digital Millennium Copyrights Act, a subpoena may be issued only to an ISP engaged in storing infringing materials on its servers or the subject of infringing activity, not to an ISP acting solely as a conduit for communications the content of which is determined by others.

Verizon argued that '§ 512(h) violates the First Amendment because it lacks sufficient safeguards to protect an internet user's ability to speak and to associate anonymously.'⁴⁵ Although the court generally agreed with Verizon, the case did not however turn on this argument but on the failure of the said subpoenas to observe an important notification requirement. In the words of the court, 'In sum, we agree with Verizon that § 512(h) does not by its terms authorize the subpoenas issued here. A § 512(h) subpoena simply cannot meet the notice requirement of § 512(c) (3) (A) (iii).'⁴⁶ The court went ahead to make an instructive *obita dictum* stating:

We are not unsympathetic either to the RIAA's concern regarding the widespread infringement of its members' copyrights, or to the need for legal tools to protect those rights. It is not the province of the courts, however, to rewrite the DMCA in order to make it fit a new and unforeseen internet architecture, no matter how damaging that development has been to the music industry or threatens being to the motion picture and software industries. The plight of copyright holders must be addressed in the first instance by the Congress...⁴⁷

Indeed, the exigencies of protecting copyrights ought not to obviate with due process, the rule of law, and all other safeguards that attach to the protection of fundamental rights. The import of the foregoing decision is that subpoenas can no longer be issued by the clerks of the courts at the instance of the copyright owners pursuant to the DMCA. The copyright owner must now file a suit in order to obtain the said subpoena. To solve the problem of the identity of the intended defendants, they are named as 'John Does' pending the outcome of the subpoenas. This also means that

⁴⁵ *Ibid.*

⁴⁶ *Ibid.*

⁴⁷ *Ibid.*

the copyright owner must also make a prima facie case of infringement before the issuance of the subpoena.

The United States District Court for the Eastern District of Pennsylvania has, in *Elektra Entertainment Group et al v. Does 1-6*,⁴⁸ taken the question of due process a step further by requiring that the unnamed defendant be given a 21 day notice before his/her ISP can release his/her personal information for the prosecution of the case. The prescribed notice gives the defendant an opportunity to challenge the subpoena in court by filing a motion to quash. The notice must also contain information on jurisdiction, the possibility of an 'out of court' settlement, and available resources for challenging the subpoena, including how to find an attorney or civil liberties organisations that may assist. In sum, the situation in the United States is such that there are no elaborate legal rules that impede online tracking and the consequent harvesting of IP addresses by the copyright owners. However, when it comes to the disclosure by the ISPs of the identity of their subscribers, the extant rule is that certain safeguards are to be observed.

4.3 *Disclosure under Directive 95/46/EC*

Within the E U, the disclosure of the identity of file sharers using their IP addresses raises issues similar to those faced by right holders during online tracking except that this time the restrictions are on the ISPs. By Article 7 (a) such disclosure will need the unambiguous consent of the file sharer/subscriber. It is to be recalled that disclosure amounts to 'processing' and the information in question, being in a computer database, involves, at the very least, partial automatic processing. However, Article 7 (c) constitutes an exception to the consent requirement in 7 (a). It provides that processing may be carried out when it is necessary for compliance with a legal obligation to which the controller is subject. This appears to be the only condition under which the ISP may safely disclose file sharers identity to right holders. What 7 (c) translates into in practice is that the right holders would need to obtain some sort of court order to compel the ISP to disclose the said information. A court order to disclose is indeed a legal obligation. Without this type of legal authorisation, disclosure by an ISP would be illegitimate under the Directive.

5 Resolution of The Clash: Safeguards

The term safeguard is used loosely here to refer to the recognition and respect of all other rights accruable to a person before lawful interference with a specific right is authorised. Procedurally speaking, it includes

⁴⁸ Civil Action No. 1241 (E.D. Pa. October 13, 2004).

observance of an individual's right to adequate notification of charges or proceedings involving him. It also includes the provision of opportunities for such persons to be heard at the said proceedings as well as opportunities to lawfully challenge same. The major consideration here is that even where the processing of personal data is legitimate or permissible in principle, the quality of the processing proper as well as the procedure leading to the processing should be safeguarded against abuse.

5.1 *Safeguards under Directive 95/46/EC*

It has been established that ISPs may disclose the identity of their subscribers when served with a properly issued court order. The requirement of a court order in itself should suffice as a safeguard seeing that the courts are already charged with the duty of safeguarding fundamental rights. It has also been established hereinabove that the Directive applies to the processing of the personal data implicated in the online tracking stage of the fight against p2p copyright infringements. However it was noted that the ECJ is likely to hold that copyright holders may legitimately process the personal data of file sharers under Article 7 (f) within clear legal boundaries. It remains then to see whether the other parts of the directive provide for these legal boundaries or safeguards. In other words, will a member state that observes all the provisions of Directive 95/46/EC be held to have provided adequate safeguards for the protection of private and family life under Article 8 ECHR? It is to be recalled that the Directive aims to give effect to Article 8 ECHR. This question will be answered in the affirmative if an examination of the directive reveals that it indeed constitutes an omnibus enactment that facilitates the definition of the scope and manner of discretion exercised pursuant to its provisions and other legislations that legitimise personal data processing by copyright holders.

5.1.1 *Supervisory Authority*

Article 28 requires each member state to establish or designate one or more public authorities to be responsible for monitoring the application of the provisions it has adopted pursuant to the Directive. The supervisory authority is to act with complete independence; and be consulted during the drawing up of administrative measures or regulations that relate to the protection of fundamental rights and freedoms connected to the processing of personal data. The supervisory authority is to be further endowed with investigative powers; effective powers of intervention, including prior checking as countenanced under Article 20; the power to engage in legal proceedings; and the power to make decisions, which may form the subject of appeals. Each supervisory authority is to be empowered to hear claims lodged by any person, or by an association representing that person. The outcome of the claim is to be communicated to the claimant. The powers of the supervisory authorities to hear claims particularly extends to

whether or not the exemptions and exceptions provided for under Article 13 apply to data processing that affects that claimant. Furthermore, the supervisory authority is to draw up periodic reports of its activities, which are to be made public.⁴⁹

5.1.2 *Obligation to Notify the Supervisory Authority*

By Article 18, the controller of personal data or his representative, if any, must notify the supervisory authority before carrying out any whole or partial automatic processing operation or set of such operations intended to serve a single purpose or several related purposes. By this provision, copyright holders or the groups thereof must notify the data protection authority in their country before proceeding with processing. It is to be noted however that exemption from, or simplification of notification provided for under paragraph 2 of Article 18 may be allowed. Accordingly, except where the state party concerned has provided for exemption or the simplification, the right holders would have to always provide notification that includes their names and addresses, the purpose of processing, a description of the category or categories of data subjects or data relating to them, the person or category of persons to whom the data will be disclosed, proposed transfer outside the community, and a description, sufficient for parliamentary assessment, of measures taken to ensure the security of the processing.⁵⁰

5.1.3 *Prior Checking*

The determination of which processing operations are likely to put the rights and freedoms of data subjects at risk would seem to be the reason for the notification requirement discussed above. Article 20 provides for just such prior checks, which the supervisory authority is mandated to conduct upon notification from the controller. Such prior checks may also be conducted in the context of legislative measures and executive measures that are based on legislative measures.⁵¹

5.1.4 *Data Quality*

The opinion has already been expressed above that the ECJ is likely to hold that right holders may process personal data within well defined legal limits. As was also suggested, the said legal limits may be seen in the Directive's provisions on the principles relating to data quality and other national provisions that prescribe due process. Other aspects of

⁴⁹ Directive 95/46/EC *Supra*, note 30, Article 28 (1) – (6).

⁵⁰ See generally Directive 95/46/EC *Supra* note 30, Article 18 and 19.

⁵¹ See *Ibid*, Article 20.

due process have been considered above, it now behoves the paper to consider these principles here. Article 6 of the Directive requires member states to provide that personal data must be processed according to a number of principles as stipulated in paragraphs (a) to (e). Paragraph (a) prescribes that processing must be fair and lawful, the 'fair collection principle'. By paragraph (b), data collection must be for a specified, explicit and legitimate purpose, the 'purpose specification principle'. The data must also not be further processed in a way incompatible with the specified purpose, the 'compatibility principle'. Paragraph (c) and (d) call for the processing of personal data to be adequate, relevant, not excessive in relation to their specified purposes, accurate, and complete, the 'data quality principle'. Paragraph (e) specifies that personal data must not be kept in a form which permits identification of data subjects for longer than is necessary, this may be termed the 'minimality principle'.⁵²

These principles clearly circumscribe what the data controller may or may not do with the data he/She is permitted to process. To the extent that data processing becomes unlawful when these principles are violated and such violation gives rise to a cause of action, they amount to safeguards against abuse. For example, the purpose specification and the compatibility principles effectively proscribe the release by ISPs of their subscribers' information to right holders without a court order. According to the Article 29 Working Party:

On the basis of the compatibility principle as well as in compliance with the confidentiality principle included in Directives 2002/58 and 95/46, data detained by ISPs processed for specific purposes including mainly the performance of a telecommunication service cannot be transferred to third parties such as right holders, except, in defined circumstances provided by law, to public law enforcement authorities.⁵³

Without the limitations imposed by the compatibility and purpose specification principles, right holders may have been able to obtain the personal data they desire from ISPs, but with the provision, along with Article 7 (a), a court order pursuant to Article 7 (c) would be called for. Furthermore, even after a supervisory authority has authorized the harvesting of IP addresses by copyright holders, the purpose specification and compatibility principles would seem to operate to limit the latitude allowed during the processing. For example, except the said right holders obtain further authorization, they may not carry out further processing by e.g. incorporating the harvested information into a

⁵² See generally L. Bygrave 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' (1998) 6 *Int. Jnl. of Law and Info. Technology*. 247.

⁵³ Working Party *Supra* note 18, p. 7.

database since this would amount to a purpose different from that for which authorization was obtained. Under the Directive, nothing stops the police from obtaining subscriber information from the ISPs since the investigation of crimes is outside the ambit of the Directive. However, other municipal provisions may make it impossible for even the police to obtain the said data without a warrant or other judicial/quasi judicial authorization.

In sum, having considered the Directive's requirement for the establishment of a supervisory authority, the notification requirement, the prior checking to be performed and the data quality principles, one cannot but agree that the Directive does provide for some serious safeguards. If these safeguards are scrupulously implemented, they will most likely satisfy the ECtHR when considering legally defined scope and manner of exercise of discretion affecting the right to private and family life. As a matter of fact, these safeguards constitute the only circumstances in which right holders may freely process the personal data in question and it is predictable that the ECJ will emphasise these when seized.

6 Conclusion

The fact that copyright holders have the right to put an end to infringements is generally well settled. This right is however not absolute. The task of this paper has been to determine whether the methods used by right holders to combat p2p copyright infringements raise privacy issues under the EC Personal Data Directive. This task has been discharged and one can safely say that the current battle methods will sometimes clash with the right to privacy of those being investigated. Two points of clash have been identified: The first is when right holders use search robots to harvest the IP addresses and other information relating to p2p file sharers. When this is done without regard to the safeguard provisions of the directive, the position of this paper is that the harvesting will amount to illegitimate processing of personal data. The second point of clash takes place offline in the various processes by which right holders seek to determine the 'real life' identities of the persons behind the harvested IP addresses. Here, when an ISP releases information relating to the identity of it's subscriber without the said subscriber's consent or an authorization in the nature of a court order, he or she will be contravening the EC personal Data Directive.

The findings of this paper may not bring much comfort to the p2p file sharer who chooses to look to data protection as a shield from infringement investigations. Any law that provides such a shield would be against public policy and thankfully the EC Personal Data Directive does not do so. The significance of the paper's findings is that it serves as a reminder to right-holder groups that while it may be permissible to process personal

data while tracking infringers, careful attention must be paid to the other parts of the directive that prescribe for safeguards. There is nothing in principle that prevents a copyright infringer who has been found liable under copyright laws from maintaining a separate action against either a copyright owner or an ISP who processed his/her personal data contrary to the directive.