Exhibit 3

Date: 20040331

Docket: T-292-04

Citation: 2004 FC 488

Ottawa, Ontario, this 31st day of March, 2004

Present: **THE HONOURABLE MR. JUSTICE von FINCKENSTEIN**

BETWEEN:

BMG CANADA INC., EMI MUSIC CANADA, A DIVISION OF EMI GROUP CANADA INC., SONY MUSIC ENTERTAINMENT (CANADA) INC., UNIVERSAL MUSIC CANADA INC., WARNER MUSIC CANADA LTD., BMG MUSIC, ARISTA RECORDS, INC., ZOMBA RECORDING CORPORATION, EMI MUSIC SWEDEN AB, CAPITOL RECORDS, INC., CHRYSALIS RECORDS LIMITED, VIRGIN RECORDS LIMITED, SONY MUSIC ENTERTAINMENT INC., SONY MUSIC ENTERTAINMENT (UK) INC., UMG RECORDINGS, INC., MERCURY RECORDS LIMITED AND WEA INTERNATIONAL INC.

Plaintiffs

and

JOHN DOE, JANE DOE AND ALL THOSE PERSONS WHO ARE INFRINGING COPYRIGHT IN THE PLAINTIFFS' SOUND RECORDINGS

Defendants

REASONS FOR ORDER AND ORDER

[1] The plaintiffs (collectively hereinafter called CRIA) are all members of Canada's recording industry and are bringing this motion to seek disclosure from five Canadian internet service providers, namely Shaw Communications Inc., Rogers Cable Communications Inc., Bell Sympatico, Telus Inc. and Vidéotron Ltée. (hereinafter collectively called ISPs) of the identity of certain customers who, it is alleged, have infringed copyright laws by illegally trading in music downloaded from the internet.

[2] The plaintiffs are unable to determine the name, address or telephone number of the 29 internet users in question as they operate under pseudonyms associated with software which they use; e.g., Geekboy @KaZaA. However, they have conducted an investigation, through which, they submit, it was discovered that these individuals used Internet Protocol addresses (IP addresses) registered with the ISPs which are the respondents to this motion. The plaintiffs are now seeking an order, pursuant to Rules 233 and 238 of the *Federal Court Rules, 1998*, SOR/98-106, to compel the ISPs to disclose the names of the customers who used the 29 IP addresses at times material to these proceedings.

[3] The plaintiffs are the largest music producers in Canada. They submit that the 29 internet users have each downloaded more than 1000 songs over which the producers have rights under the *Copyright Act*, R.S., 1985, c. C-42, onto their home computers.

[4] The operation of the peer-to-peer ("P2P") file-sharing programs Morpheus and Grokster was described in *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster*, 259 F. Supp.2d 1029 (C.D. Cal. 2003) at 1032-1033 as follows:

> In both cases, the software can be transferred to the user's computer, or "downloaded," from servers operated by Defendants. Once installed, a user may elect to "share" certain files located on the user's computer, including, for instance, music files, video files, software applications, e-books and text files. When launched on the user's computer, the software automatically connects to a peer-to-peer network... and makes any shared files available for transfer to any other user currently connected to the same peer-to-peer network.
>
> Both the Morpheus and Grokster software provide a range of means through which a user may search through the respective pool of shared files. For instance, a user can select to search only among audio files, and then enter a keyword, title, or artist search. Once a search commences, the software displays a list (or partial list) of users who are currently sharing files that match the search criteria, including data such as the estimated time required to transfer each file.
>
> The user may then click on a specific listing to initiate a direct transfer from the source computer to the requesting user's computer. When the transfer is complete, the requesting user and source user have identical copies of the file, and the requesting user may also start sharing the file with others. Multiple transfers to other users ("uploads"), or from other users ("downloads"), may occur simultaneously to and from a single user's computer.

The file-sharing systems in issue in this case, KaZaA and iMesh, work basically on the same principles.

[5] The plaintiffs submit that this form of file-sharing constitutes an infringement of their rights over certain music under the *Copyright Act*. The ISPs, other than Vidéotron, raise various objections to the order.

[6] Two public interest groups, the Canadian Internet Policy and Public Interest Clinic (CIPPIC) and Electronic Frontier Canada (EFC), were granted intervener status for the purpose of making arguments.

[7] Rules 232 and 238 and the relevant portion of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 (PIPEDA) and the *Copyright Act* are attached as Annex A.

ISSUES

[8] This motion raises three issues:

1. What legal test should this Court apply?
2. Have the plaintiffs met the test?
3. If an order is issued, what should be the scope and terms of such order?

Common ground

[9] Before addressing these issues it should be noted that all of the parties to this motion agreed on the following points.

- ISP account holders have an expectation that their identity will be kept private and confidential. This expectation of privacy is based on both the terms of their account

agreements with the ISPs and sections 3 and 5 of the *Personal Information Protection and Electronic Documents Act. (PIPEDA)*

- The exceptions contained in PIPEDA apply in this case and an ISP by virtue of s. 7(3)(c) of PIPEDA may disclose personal information without consent pursuant to a court order.

Issue 1. ***What legal test should this Court apply?***

[10] *Norwich Pharmacal Co. v. Customs and Excise Commissioners*, [1974] A.C. 133 and *Glaxo Welcome PLC v. Canada (Minister of National Revenue)* (1998), 81 C.P.R. (3rd) 372 have established that where a potential plaintiff seeks pre-action discovery in order to ascertain the identity of a defendant he can do so by way of an equitable bill of discovery. However, once an action has been started, as in the instance case (albeit by naming John and Jane Doe as defendants), the plaintiff has to resort to Rules 233 or 238 instead of resorting to an equitable bill of discovery.

[11] The rationale for such a procedure was succinctly expressed by Lord Reid in *Norwich, supra* on page 175 where he stated:

> On the whole I think they favour the appellants, and I am particularly impressed by the views expressed by Lord Romilly M.R. and Lord Hatherley L.C. in Upmann v. Elkan (1871) L.R. 12 Eq. 140; 7 Ch.App. 130. They seem to me to point to a very reasonable principle that if through no fault of his own a person gets mixed up in the tortious acts of others so as to facilitate their wrong-doing he may incur no personal liability but he comes under a duty to assist the person who has been wronged by giving him full information and disclosing the identity

> of the wrongdoers. I do not think that it matters whether he became so mixed up by voluntary action on his part or because it was his duty to do what he did. It may be that if this causes him expense the person seeking the information ought to reimburse him. But justice requires that he should co-operate in righting the wrong if he unwittingly facilitated its perpetration.

[12] In *Glaxo Welcome PLC, supra* which followed *Norwich, supra* and applied it in Canada, Stone J.A. described the preconditions for granting such relief on page 387 where he stated:

> While the bill of discovery as an equitable remedy is discretionary in nature, the House of Lords in Norwich Pharmacal, supra, enumerated a number of considerations which are key to determining whether to grant it. Lord Cross of Chelsea stated at page 199 that important factors include:
>
> > . . . the strength of the applicant's case against the unknown alleged wrongdoer, the relation subsisting between the alleged wrongdoer and the respondent, whether the information could be obtained from another source, and whether the giving of the information would put the respondent to trouble which could not be compensated by the payment of all expenses by the applicant.
>
> Lord Kilbrandon echoed many of these considerations at page 205:
>
> > In my opinion, accordingly, the respondents, in consequence of the relationship in which they stand, arising out of their statutory functions, [to the appellants and their rights of property], can properly be ordered by the court to disclose to the appellants the names of persons whom the appellants bona fide believe to be infringing these rights, this being their only practicable source of information as to whom they should sue, subject to any special right of exception which the respondents may qualify in respect of their position as a department of state.
>
> It seems to me that the requirement that the appellants have a bona fide claim against the alleged wrongdoers is intended to ensure that actions for a bill of discovery are not brought frivolously or without any justification. Likewise, the criterion that the appellants must share some sort of relationship with the respondents may be conceptualized as an alternative formulation of the principle that a bill of discovery may not be issued against a mere witness or disinterested bystander to the alleged misconduct. I would therefore characterize these two considerations as threshold requirements for obtaining an equitable bill of discovery.

The above-quoted passages from the reasons of Lord Cross of Chelsea and Lord Kilbrandon also signal that a basic condition for granting a bill of discovery is that the person from whom discovery is sought must be the only practical source of information available to the appellants. Lord Reid underscored the importance of this criterion at page 174, where he made the following finding:

> Here if the information in the possession of the respondents cannot be made available by discovery now, no action can ever be begun because the appellants do not know who are the wrongdoers who have infringed their patent. So the appellants can never get the information.

Last, the House of Lords took into account the public interests both in favour and against disclosure. Lord Reid maintained at page 175 that his task was to "weigh the requirements of justice to the appellants against the considerations put forward by the respondents as justifying non-disclosure". In his view, the Commissioners were obliged to disclose the names of the importers "unless there is some consideration of public policy which prevents that". The House of Lords approached this balancing exercise from a variety of perspectives. The Law Lords recognized that because of the statutory bar on disclosure of the importers' names, there may be an overriding public interest in preserving the confidentiality of the information. They acknowledged that the importers may accordingly have an expectation that their names would remain confidential. The public interest in non-disclosure was also examined from the standpoint of the state and its stake in ensuring the effective administration and enforcement of the legislative scheme at issue. At the same time, the Law Lords appreciated that disclosure of the names of the importers may very well serve the public interest in the fair and efficient administration of justice. As Viscount Dilhorne stated at page 188:

> Subject to the public interest in protecting the confidentiality of information given to Customs, in my opinion it is clearly in the public interest and right for the protection of patent holders, where the validity of the patent is accepted and the infringement of it not disputed, that they should be able to obtain by discovery the names and addresses of the wrongdoers from someone involved but not a party to the wrongdoing.

[13] I read the *Norwich* and *Glaxco Wellcome* cases as establishing that the test for granting an equitable bill of discovery involves the following five criteria:

a) the applicant must establish a *prima facie* case against the unknown alleged wrongdoer;

b) the person from whom discovery is sought must be in some way involved in the matter under dispute, he must be more than an innocent bystander;

c) the person from whom discovery is sought must be the only practical source of information available to the applicants;

d) the person from whom discovery is sought must be reasonably compensated for his expenses arising out of compliance with the discovery order in addition to his legal costs;

e) the public interests in favour of disclosure must outweigh the legitimate privacy concerns.

[14] I can think of no reason why the same principles should not also apply to an application brought under Rule 238 in a John Doe action. The requirement for service under subsection 2 of Rule 238 can and, of course, would be waived by a court in such an action pursuant to Rule 55.

[15] The plaintiffs have also brought this motion under Rule 233, however this Rule presupposes the existence of specified documents. The definition of a document contained in Rule 222, in my view, is not broad enough to cover the creation of documents not normally held by a party nor retrievable through computer systems used by a party in its ordinary business. In this case, documents do not pre-

exist which link an IP address to the customer of an ISP. Documents would, of course, be generated should an ISP be compelled to make this connection; however, this is not something contemplated by Rule 233. In short, the purpose of Rule 233 is to compel the disclosure, but not the very creation of documents.

Criterion a: the applicant must establish a *prima facie* case against the unknown alleged wrongdoer

[16] There are three deficiencies in the *prima facie* case advanced by the plaintiffs:

I) The affidavit is deficient as to content.

[17] The affidavits of Gary Millin on which the plaintiffs rely state that he was, at material times, the President of MediaSentry Inc., a company which provides online anti-privacy protection. This company was hired by the Canadian Recording Industry Association to investigate file-sharing of songs over which the plaintiffs have copyrights. In his affidavit, Mr. Millin described MediaSentry's findings with regard to the file-sharing activities of the 29 unnamed defendants. The major portions of these affidavits are based upon information which Mr. Millin gained from his employees. Accordingly, they consist largely of hearsay. Pursuant to Rule 81(1), hearsay and other forms of information gained on belief may be admissible provided that the grounds for the belief are stated. Beyond stating in cross-examination that, as President of MediaSentry "a company of 20 to 25 employees", he had "general oversight for

the business and particular strategy" *(Cross- examination of Millin, pp.6 and 8, lines 16 and 18 respectively)*, Mr. Millin gives no reason for his beliefs. This is insufficient. As stated by Heald J.A. in *Maligne Building Ltd. v. Canada* (1980), 37 NR 562 at para. 2:

> Where affidavit evidence is founded on information and belief it is essential to state the source of the information.

[18] Moreover, Rule 81(2) provides:

> Where an affidavit is made on belief, an adverse inference may be drawn from the failure of a party to provide evidence of persons having personal knowledge of the material facts.

It seems clear that there are other MediaSentry employees would have been in a better position to swear the affidavits in question and to answer the respondents' questions on cross-examination. At the very least, Mr. Millin should have identified the employees who conducted the work, stated their qualifications and explained how they conveyed the result of their investigations to him. Thurlow A.C.J. stated, in respect of Rule 81, in *The Queen v. A. & A. Jewellers Ltd.*, [1978] 1 F.C. 479, at page 480:

> The Court is entitled to the sworn statement of the person who has personal knowledge of the facts when he is available. The second part of the Rule is merely permissive and is for use only when the best evidence, that is to say the oath of the person who knows, is for some acceptable or obvious reason not readily obtainable. (emphasis added)

There is no such reason given in either Mr. Millin's affidavits or in his cross-examination for the contravention of the best evidence rule.

[19] Mr. Millin also testified that his company provided a service called MediaDecoy which distributes bogus or inoperative files over the internet. People downloading these files think incorrectly that they are music files. The files are made to look like real music files, but they are inoperative. When he was asked whether he could tell whether any of the files allegedly copied from the alleged infringers were MediaDecoy files, Mr. Millin stated that he had not listened to any of the files copied from the alleged infringers and that listening to the files was not work that his firm was contracted to do or the "process that we set up with CRIA" *(Millin cross-examination, QQ 107-107, 189-196)*. This kind of remote evidence in no way qualifies under Rule 81. There is, thus, no evidence before the Court as to whether or not the files offered for uploading are infringed files of the plaintiffs.

ii) There is no evidence of connection between the pseudonyms and the IP addresses.

[20] As discussed above, the plaintiffs would like the ISPs to furnish the names of the account holders of certain IP addresses at certain times. However, neither the affidavits nor the cross-examination of Mr. Millin provide clear and comprehensive evidence as to how the pseudonyms of the KaZaA or iMesh users were linked to the IP addresses identified by MediaSentry. For example, with regards to one of the 29 pseudonyms, Mr. Millin stated in his affidavit:

> MediaSentry also determined that Geekboy@KaZaA's IP at the time of its investigation was 24.84.179.98. The American Registry for Internet Numbers ("ARIN"), a non-profit organization that assigns IP addresses to Internet Service Providers ("ISPs"), maintains a public database of IP addresses at www.arin.net.

> This database indicates that ARIN has assigned IP address 24.84.179.98 to Shaw Communications Inc.....
>
> (Affidavit of Mr. Millin in Motion Materials Related to Shaw, para. 24)

There is no evidence explaining how the pseudonym "Geekboy@KaZaA" was linked to IP address 24.84.179.98 in the first place. Without any evidence at all as to how IP address 24.84.179.98 has been traced to Geekboy@KaZaA, and without being satisfied that such evidence is reliable, it would be irresponsible for the Court to order the disclosure of the name of the account holder of IP address 24.84.179.98 and expose this individual to a law suit by the plaintiffs.

iii) no evidence of infringement of copyright.

[21] The plaintiffs submit in paragraph 84 of their written representations that their evidence shows that the alleged infringers:

a. installed the peer-to-peer application on their computers (Millin, para. 10);

b. copied files to "shared directories" on their computers (Millin, para.9);

c. used ISP services to connect their computers to the Internet (Millin, para.16);

d. ran the peer-to-peer application on their computers while in the Internet (Millin, para. 16); and

e. made the files in the shared directories available for copying, transmission and distribution to any one of millions of users of the peer-to-peer service (Millin, para. 22).

[22] They submit in paragraph 102 of their written representations that such activity amounts to infringement of the *Copyright Act* on the following grounds:

a. ***reproduction*** of sound recordings by the alleged infringers (s. 18(1) and s. 27(1));

b. ***authorization*** of the reproduction of the sound recordings (s. 18(1) and s. 27(1));

c. ***distribution*** of unauthorized copies of the sound recordings to such an extent as to affect prejudicially the plaintiffs (s. 27(2)(b)), and

d. ***possession*** of unauthorized copies, which the alleged infringers knew or ought to have known were infringing, for the purpose of distribution, as set out above (s. 27(2)(d)).

[23] These submissions have to be examined in light of the nature of copyright law. Copyright law can be invoked by owners only to the extent explicitly set forth in the statute. A court cannot infer or provide rights that are not provided for in the statute. As Estey J. stated in *Compo Co. v. Blue Crest Music Inc.*, [1980] 1 S.C.R. 357 at 372-373 :

> ....copyright law is neither tort law nor property law in classification, but is statutory law. It neither cuts across existing rights in property or conduct nor falls between rights and obligations heretofore existing in the common law. Copyright legislation simply creates rights and obligations upon the terms and in the circumstances set out in the statute. This creature of statute has been known to the law of England at least since the days of Queen Anne when the first copyright statute was passed. It does not assist the interpretive analysis to import tort concepts. The legislation speaks for itself and the actions of the appellant must be measured according to the terms of the statute.

The Court thus must look at the plaintiffs' submissions through the lense of *Compo Co., supra.*

[24] Section 80 (1) of the *Copyright Act* provides as follows:

80. (1) Subject to subsection (2), the act of reproducing all or any substantial part of (a) a musical work embodied in a sound recording, ...	80. (1) Sous réserve du paragraphe (2), ne constitue pas une violation du droit d'auteur protégeant tant l'enregistrement sonore que l'oeuvre musicale ou la prestation d'une oeuvre
onto an audio recording medium for the private use of the person who makes the copy does not constitute an infringement of the copyright in the musical work, the performer's performance or the sound recording.	musicale qui le constituent, le fait de reproduire pour usage privé l'intégralité ou toute partie importante de cet enregistrement sonore, de cette oeuvre ou de cette prestation sur un support audio.

[25] Thus, downloading a song for personal use does not amount to infringement. See *Copyright Board of Canada, Private Copying 2003-2004 decision,* 12 December 2003 at page 20.

[26] No evidence was presented that the alleged infringers either distributed or authorized the reproduction of sound recordings. They merely placed personal copies into their shared directories which were accessible by other computer user via a P2P service.

[27] As far as authorization is concerned, the case of *CCH Canada Ltd v. Law Society of Canada,* 2004 SCC 13, established that setting up the facilities that allow copying does not amount to authorizing infringement. I cannot see a real difference between a library that places a photocopy

machine in a room full of copyrighted material and a computer user that places a personal copy on a shared directory linked to a P2P service. In either case the preconditions to copying and infringement are set up but the element of authorization is missing. As Chief Justice McLachlin said in *CCH, supra*:

> "Authorize" means to "sanction, approve and countenance": Muzak Corp. v. Composers, Authors and Publishers Association of Canada Ltd., [1953] 2 S.C.R. 182, at p. 193; De Tervagne v. Beloeil (Town), [1993], 3 F.C. 227 (F.C.T.D.). Countenance in the context of authorizing copyright infringement must be understood in its strongest dictionary meaning, namely, "give approval to, sanction, permit, favour, encourage": see The New Shorter Oxford English Dictionary (1993), vol. 1, at p. 526. Authorization is a question of fact that depends on the circumstances of each particular case and can be inferred from acts that are less than direct and positive, including a sufficient degree of indifference: CBS Inc. v. Ames Records & Tapes Ltd., [1981] 2 All E.R. 812 (Ch.D.), at pp. 823-24. However, a person does not authorize infringement by authorizing the mere use of equipment that could be used to infringe copyright. Courts should presume that a person who authorizes an activity does so only so far as it is in accordance with the law: Muzak, supra. This presumption may be rebutted if it is shown that a certain relationship or degree of control existed between the alleged authorizer and the persons who committed the copyright infringement: Muzak, supra; De Tervagne, supra: see also, J. S. McKeown, Fox Canadian Law of Copyright and Industrial Designs, 4th ed. (looseleaf), at p. 21-104 and P. D. Hitchcock, "Home Copying and Authorization" (1983), 67 C.P.R. (2d) 17, at pp. 29-33.

[28] The mere fact of placing a copy on a shared directory in a computer where that copy can be accessed via a P2P service does not amount to distribution. Before it constitutes distribution, there must be a positive act by the owner of the shared directory, such as sending out the copies or advertising that they are available for copying. No such evidence was presented by the plaintiffs in this case. They merely presented evidence that the alleged infringers made copies available on their shared drives. The exclusive right to make available is included in the *World Intellectual Property Organization Performances and Phonograms Treaty*, (WPPT), 20/12/1996 (CRNR/DC/95, December 23,

1996), however that treaty has not yet been implemented in Canada and therefore does not form part of Canadian copyright law.

[29] Lastly, while the plaintiffs allege that there was secondary infringement contrary to s. 27(2) of the *Copyright Act*, they presented no evidence of knowledge on the part of the infringer. Such evidence of knowledge is a necessary condition for establishing infringement under that section.

Criterion b: the person from whom discovery is sought must be in some way involved in the matter under dispute, he must be more than an innocent bystander

[30] In the instant case the plaintiffs meet the requirements of point d) in paragraph 22 above. As providers of access to the internet, the ISPs are definitively involved with the alleged infringers. They are not mere bystanders. They are the means by which downloaders and uploaders access the internet and get in touch with each other.

Criterion c: the person from whom discovery is sought must be the only practical source of information available to the applicants

[31] In this case, the alleged wrongdoers used software called KaZaA, KaZaA Lite or iMesh which they downloaded from websites by those names. The affidavits of Gary Millin and Kathy Yonekura do not at any point mention who operates these websites, where they are located or whether the name of

the pseudonyms can be obtained from the operators of these websites. In the absence of such evidence the Court cannot make a determination as to whether or not the ISPs are the only practical source of information available to the plaintiffs.

Criterion d: the person from whom discovery is sought must be reasonably compensated for his expenses arising out of compliance with of the discovery order in addition to his legal costs

[32] The affidavits filed by Telus, Shaw, Rogers, Bell and EFC reveal that it is not an easy task to provide the name and address of the account holder who used a specific IP address at a given time.

[33] For instance, David Shrimpton of Telus describes the process as follows:

> 16. To attempt to obtain that information requested, TELUS employees will be required to conduct searches of at least three different databases and cross-reference the information found, to locate the likely account holder. This process is not done in the normal course of business and thus there are no existing lists, files, records, or documents containing the information requested. In addition, none of the TELUS staff would know the information requested as a result of their normal duties. TELUS does not monitor the content of what account holders access on the Internet.
>
> 17. The only way to locate the account that accessed the Internet using the IP address in question would be to cross-reference the IP address at the date, time, network and time zone to a database of MAC addresses and then cross-reference the MAC address with the account database, assuming that the information still exists and is recoverable. As discussed below, the more historic a search is, the less reliable the information will be, as records are kept in different ways for different systems.
>
> 18. TELUS provides Internet service primarily in Alberta and British Columbia but has accounts in some of the other provinces and territories as well. TELUS has 750,000 individual Internet account holders and provides Internet service to 85,000 institutions, government departments and corporations. These numbers only reflect our consumer and small business customers.

19. TELUS has a certain number of IP addresses allocated to it by the American Registry for Internet Numbers ("ARIN"). There are, however, fewer IP addresses than accounts. This is true for all ISPs. The IP system is predicated on the assumption that all potential users will not want to access the Internet at the same time. Accordingly, most IP addresses are dynamic, which means that they are not associated consistently with any particular personal computer ("PC") or Internet access account. Instead as a customer accesses the Internet, the hardware connection, to which the person's PC is connected, "calls" for an IP address and one is "assigned" to it temporarily by the system. Accordingly, an IP address may not be associated with any account for very long. An IP address can be reallocated to several users in the space of a few hours. Because the frequency of visits and duration of time spent online differs from user to user, the IP addresses are not assigned to the MAC addresses sequentially. As a result of this functionality, IP addresses are not associated with any one account holder nor are they allocated in any predetermined pattern (the use of the term "IP address" is perhaps confusing in the conventional sense because it is not an address, as one understands a house to have an address). It is therefore not possible to directly identify an account holder merely from an IP address. Moreover, searching for the IP address is not straightforward.

20. To complicate matters, the PC does not itself have an address, but rather the hardware connection, *i.e.*, the router or network adaptor, through which the PC gains access to the Internet had an embedded address that was assigned to it when it accessed the Internet for the first time. This is called the MAC address and it is an address associated with the hardware connection not the PC. This distinction is important, particularly when the hardware connection provides access to multiple PCs through the use of a Local Area Network ("LAN"), as discussed below.

21. Accordingly, for TELUS to determine the account holder, we would first have to determine which MAC address was assigned the IP address in question at the particular point in time.

22. Please note that TELUS can never identify the "user", *i.e.*, the person actually using the computer at the time of the alleged infringement. TELUS can only identify the person who opened up the TELUS account associated with the MAC address. As will be discussed below, the account holder and the user are not always the same, or even known to each other. With respect to the account holder, if the request is made within 30 days of when the Internet was accessed for the peer-to-peer sharing activity, TELUS has a good chance of identifying the account (depending on the particular TELUS Internet system the customer was using). However, for requests concerning customer activity 30 days or more before the request, the information becomes less reliable to the point of being non-existent.

[34] Without going into the technical details furnished by each ISP, one can draw the following overall conclusions from the evidence tendered by the ISPs with regard to such information:

- this is not information routinely kept by the ISPs but information that must be specifically retrieved from their data banks;
- the older the information is, the more difficult it will be to retrieve it. The data may be on back-up tapes or may no longer be kept depending upon the age of the information;
- the older the information, the more unreliable the result that will be produced by trying to retrieve the data;
- it may be impossible, due to the passage of time, to link some IP addresses to account holders;
- at best the ISPs will generate the name of the account holders; however, they can never generate the name of the actual computer users. An IP address, for instance, can lead to the name of an account holder, but that account holder could be an institution and/or may be linked to a local area network of many users.

[35] Clearly the process that is sought to be imposed on the ISPs would be costly and would divert their resources from other tasks. Given that the ISPs are in no way involved in any alleged infringement, they would need to be reimbursed for their reasonable costs for furnishing the names of account holders, as well as the legal costs of responding to this motion.

Criterion e: the public interests in favour of disclosure must outweigh the legitimate privacy concerns

[36] It is unquestionable but that the protection of privacy is of utmost importance to Canadian society. In the words of Lamer J. in *R. v. Dyment*, [1988] 2 S.C.R. 417 (S.C.C.):

> Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection, but it also has profound significance for the public order.

[37] In respect of the internet specifically, Wilkins J. in *Irwin Toy v. Doe* (2000), 12 C.P.C. (5th) 103 (Ont. S.C.J.) stated at paras. 10-11:

> Implicit in the passage of information through the internet by utilization of an alias or pseudonym is the mutual understanding that, to some degree, the identity of the source will be concealed. Some internet service providers inform the users of their services that they will safeguard their privacy and/or conceal their identity and, apparently, they even go so far as to have their privacy policies reviewed and audited for compliance. Generally speaking, it is understood that a person's internet protocol address will not be disclosed. Apparently, some internet service providers require their customers to agree that they will not transmit messages that are defamatory or libellous in exchange for the internet service to take reasonable measures to protect the privacy of the originator of the information.
>
> In keeping with the protocol or etiquette developed in the usage of the internet, some degree of privacy or confidentiality with respect to the identity of the internet protocol address of the originator of a message has significant safety value and is in keeping with what should be perceived as being good public policy. As far as I am aware, there is no duty or obligation upon the internet service provider to voluntarily disclose the identity of an internet protocol address, or to provide that information upon request.

[38] Parliament has also recognized the need to protect privacy by enacting PIPEDA, which has as one of its primary purposes the protection of an individual's right to control the collection, use and disclosure of personal information by private organizations (section 3).

[39] However while the law protects an individual's right to privacy, privacy cannot be used to protect a person from the application of either civil or criminal liability. Accordingly, there is no limitation in PIPEDA restricting the ability of the Court to order production of documents related to their identity. Section 7(3)(c) allows disclosure without consent if such disclosure is:

> c) required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records.
> (emphasis added).

[40] Thus, both PIPEDA as well as the test set out in *Norwich/Glaxco*, require the Court to balance privacy rights against the rights of other individuals and the public interest.

[41] This motion is not a novel proceeding. In the past, third parties have been compelled to disclose documents identifying the name and address of a defendant previously identified solely by an Internet Protocol address. In no case have privacy or other concerns weighing against disclosure outweighed the interest in obtaining documents and information necessary to identify the defendants. See: *Irwin Toy v. Doe* (2000), 12 C.P.C. (5th) 103 (Ont. S.C.J.); *Ontario First Nations Limited Partnership v. John Doe* (3 June 2002) (Ont.S.C.J.); *Canadian Blood Services/Société Canadienne du Sang v.*

John Doe (June 17, 2002) (Ont. S.C.J.); *Wa'el Chehab v. John Doe* (October 3, 2003) (Ont. S.C.J.); *Kibale v. Canada,* [1991] F.C.J. No. 634 (QL) (FC); *Loblaw Companies Ltd. v. Aliant Telecom Inc. and Yahoo* [2003] N.B.J. No.208 (N.B.Q.B.), online: QL (NBJ).

[42] In this case, the plaintiffs have a legitimate copyright in their works and are entitled to protect it against infringement. However before making the order, the Court evidently must be satisfied that the information about to be disclosed is reliable and should restrict disclosure to the minimum required for the plaintiffs to identify an alleged defendant. Any order made should also, having in mind the privacy interests of the defendants, be accompanied by restrictions and confidentiality orders as the Court sees appropriate. All of the ISPs have indicated that they can produce the required information if requested in a timely fashion. In this case the evidence was gathered in October, November and December 2003. However, the notice of motion requesting disclosure by the ISPs was not filed until February 11, 2003. This clearly makes the information more difficult to obtain, if it can be obtained at all, and decreases its reliability. No explanation was given by the plaintiffs as to why they did not move earlier than February 2003. Under these circumstances, given the age of the data, its unreliability and the serious possibility of an innocent account holder being identified, this Court is of the view that the privacy concerns outweigh the public interest concerns in favour of disclosure.

Issue 2: ***Have the plaintiffs met the test?***

[43] On the basis of the foregoing, it is obvious that in my mind the plaintiffs have not:

- made out a *prima facie* case (their affidavit evidence is deficient, they have not made a causal link between P2P pseudonyms and IP addresses and they have not made out a *prima facie* case of infringement);
- established that the ISPs are the only practical source for the identity of the P2P pseudonyms; and
- established that the public interest for disclosure outweighs the privacy concerns in light of the age of the data.

Consequently, they have not met the test set out in paragraph 13 above.

Issue 3. ***If an order is issued, what should be the scope and terms of such order?***

[44] If an order had been issued in this case, certain restrictions would have been necessary in order to protect the privacy interests of the yet unnamed defendants. First, the order would have limited the use to which the identities might be used to the within proceedings. I see no reason why the implied undertaking rule might have been waived as requested by the plaintiffs. The invasion of privacy should always be as limited as possible. As the plaintiffs asked for the defendants' names so that they could be substituted for John and Jane Doe, the names should only have been granted for that purpose.

[45] Second, to further minimize the invasion of privacy of the ISP account holders, the order would have provided that only the internet pseudonyms be added as defendants in the statement of claim. An annex (subject to a confidentiality order) would have been added to the statement of claim relating each pseudonym to the name and address of an ISP account holder.

[46] Finally, the order would not have required the ISPs to provide an affidavit in support of their findings. The mere disclosure of the defendants' names and last known addresses would have been sufficient in order to allow the plaintiffs to proceed with their action.

[47] Given my finding in respect of issue 2, this motion cannot succeed.

ORDER

1. This motion is denied.
2. All respondent ISPs shall have their costs in this matter.
3. There will be no award as to costs with respect to the interveners.

"K. von Finckenstein"

Judge

Annex A

Federal Court Rules, 1998, SOR/98-106

41.(1) Subject to subsection (4), on receipt of a written request, the Administrator shall issue, in Form 41, a subpoena for the attendance of a witness or the production of a document or other material in a proceeding.

41.(1) Sous réserve du paragraphe (4), sur réception d'une demande écrite, l'administrateur délivre un subpoena, selon la formule 41, pour contraindre un témoin à comparaître ou à produire un document ou des éléments matériels dans une instance.

233.(1) On motion, the Court may order the production of any document that is in the possession of a person who is not a party to the action, if the document is relevant and its production could be compelled at trial.

233.(1) La Cour peut, sur requête, ordonner qu'un document en la possession d'une personne qui n'est pas une partie à l'action soit produit s'il est pertinent et si sa production pourrait être exigée lors de l'instruction.

238. (1) A party to an action may bring a motion for leave to examine for discovery any person not a party to the action, other than an expert witness for a party, who might have information on an issue in the action.

238.(1) Une partie à une action peut, par voie de requête, demander l'autorisation de procéder à l'interrogatoire préalable d'une personne qui n'est pas une partie, autre qu'un témoin expert d'une partie, qui pourrait posséder des renseignements sur une question litigieuse soulevée dans l'action.

...

...

(3) The Court may, on a motion under subsection (1), grant leave to examine a person and determine the time and manner of conducting the examination, if it is satisfied that
(a) the person may have information on an issue in the action;
(b) the party has been unable to obtain the information informally from the person or from another source by any other reasonable means;
(c) it would be unfair not to allow the party an opportunity to question the person before trial; and
(d) the questioning will not cause undue delay, inconvenience or expense to the person or to the other parties.

(3) Par suite de la requête visée au paragraphe (1), la Cour peut autoriser la partie à interroger une personne et fixer la date et l'heure de l'interrogatoire et la façon de procéder, si elle est convaincue, à la fois :
a) que la personne peut posséder des renseignements sur une question litigieuse soulevée dans l'action;
b) que la partie n'a pu obtenir ces renseignements de la personne de façon informelle ou d'une autre source par des moyens raisonnables;
c) qu'il serait injuste de ne pas permettre à la partie d'interroger la personne avant l'instruction;
d) que l'interrogatoire n'occasionnera pas de retards, d'inconvénients ou de frais déraisonnables à la personne ou aux autres parties.

Personal Information Protection and Electronic Documents Act, R.S., 2000, c. 5.

3. The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

3. La présente partie a pour objet de fixer, dans une ère où la technologie facilite de plus en plus la circulation et l'échange de renseignements, des règles régissant la collecte, l'utilisation et la communication de renseignements personnels d'une manière qui tient compte du droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent et du besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

4.(3) Every provision of this Part applies despite any provision, enacted after this subsection comes into force, of any other Act of Parliament, unless the other Act expressly declares that that provision operates despite the provision of this Part.

4.(3) Toute disposition de la présente partie s'applique malgré toute disposition — édictée après l'entrée en vigueur du présent paragraphe — d'une autre loi fédérale, sauf dérogation expresse de la disposition de l'autre loi.

5.(3) An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

5.(3) L'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

7.(3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is

...

(*c*) required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records;

...

(*d*) made on the initiative of the organization to an investigative body, a government institution or a part of a government institution and the organization

(i) has reasonable grounds to believe that the information relates to a breach of an agreement or a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed,

...

(*e*) made to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in writing without delay of the disclosure;

...

(*h.2*) made by an investigative body and the disclosure is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province; or

(*i*) required by law.

7.(3) Pour l'application de l'article 4.3 de l'annexe 1 et malgré la note afférente, l'organisation ne peut communiquer de renseignement personnel à l'insu de l'intéressé et sans son consentement que dans les cas suivants :

...

c) elle est exigée par assignation, mandat ou ordonnance d'un tribunal, d'une personne ou d'un organisme ayant le pouvoir de contraindre à la production de renseignements ou exigée par des règles de procédure se rapportant à la production de documents;

...

d) elle est faite, à l'initiative de l'organisation, à un organisme d'enquête, une institution gouvernementale ou une subdivision d'une telle institution et l'organisation, selon le cas, a des motifs raisonnables de croire que le renseignement est afférent à la violation d'un accord ou à une contravention au droit fédéral, provincial ou étranger qui a été commise ou est en train ou sur le point de l'être

...

e) elle est faite à toute personne qui a besoin du renseignement en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de toute personne et, dans le cas où la personne visée par le renseignement est vivante, l'organisation en informe par écrit et sans délai cette dernière;

...

h.2) elle est faite par un organisme d'enquête et est raisonnable à des fins liées à une enquête sur la violation d'un accord ou la contravention du droit fédéral ou provincial;

i) elle est exigée par la loi.

PIPEDA: Schedule 1 - Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96

4.3 The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate
...

4.3 Toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.

4.3.1 Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection
...

4.3.1 Il faut obtenir le consentement de la personne concernée avant de recueillir des renseignements personnels à son sujet et d'utiliser ou de communiquer les renseignements recueillis. Généralement, une organisation obtient le consentement des personnes concernées relativement à l'utilisation et à la communication des renseignements personnels au moment de la collecte.
...

4.3.5 In obtaining consent, the reasonable expectations of the individual are also relevant
...

4.3.5 Dans l'obtention du consentement, les attentes raisonnables de la personne sont aussi pertinentes.
...

4.5 Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law
...

4.5 Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'exige.
...

Copyright Act, R.S, 1985, c. C-42.

(2) It is an infringement of copyright for any person to

(a) sell or rent out,
(b) distribute to such an extent as to affect prejudicially the owner of the copyright,
(c) by way of trade distribute, expose or offer for sale or rental, or exhibit in public,
(d) possess for the purpose of doing anything referred to in paragraphs (a) to (c),
...

(2) Constitue une violation du droit d'auteur l'accomplissement de

...
a) la vente ou la location;
b) la mise en circulation de façon à porter préjudice au titulaire du droit d'auteur;
c) la mise en circulation, la mise ou l'offre en vente ou en location, ou l'exposition en public, dans un but commercial;
d) la possession en vue de l'un ou l'autre des actes visés aux alinéas a) à c);
...

34. (1) Where copyright has been infringed, the owner of the copyright is, subject to this Act, entitled to all remedies by way of injunction, damages, accounts, delivery up and otherwise that are or may be conferred by law for the infringement of a right.

34. (1) En cas de violation d'un droit d'auteur, le titulaire du droit est admis, sous réserve des autres dispositions de la présente loi, à exercer tous les recours — en vue notamment d'une injonction, de dommages-intérêts, d'une reddition de compte ou d'une remise — que la loi accorde ou peut accorder pour la violation d'un droit.

37. The Federal Court has concurrent jurisdiction with provincial courts to hear and determine all proceedings, other than the prosecution of offences under section 42 and 43, for the enforcement of a provision of this Act or of the civil remedies provided by this Act.

37. La Cour fédérale, concurremment avec les tribunaux provinciaux, connaît de toute procédure liée à l'application de la présente loi, à l'exclusion des poursuites visées aux articles 42 et 43.

80. (1) Subject to subsection (2), the act of reproducing all or any substantial part of
(a) a musical work embodied in a sound recording,
(b) a performer's performance of a musical work embodied in a sound recording, or
(c) a sound recording in which a musical work, or a performer's performance of a musical work, is embodied
onto an audio recording medium for the private use of the person who makes the copy does not constitute an infringement of the copyright in the musical work, the performer's performance or the sound recording.

80. (1) Sous réserve du paragraphe (2), ne constitue pas une violation du droit d'auteur protégeant tant l'enregistrement sonore que l'oeuvre musicale ou la prestation d'une oeuvre musicale qui le constituent, le fait de reproduire pour usage privé l'intégralité ou toute partie importante de cet enregistrement sonore, de cette oeuvre ou de cette prestation sur un support audio.

(2) Subsection (1) does not apply if the act described in that subsection is done for the purpose of doing any of the following in relation to any of the things referred to in paragraphs (1)(a) to (c):
(a) selling or renting out, or by way of trade exposing or offering for sale or rental;
(b) distributing, whether or not for the purpose of trade;
(c) communicating to the public by telecommunication; or
(d) performing, or causing to be performed, in public.

(2) Le paragraphe (1) ne s'applique pas à la reproduction de l'intégralité ou de toute partie importante d'un enregistrement sonore, ou de l'oeuvre musicale ou de la prestation d'une oeuvre musicale qui le constituent, sur un support audio pour les usages suivants :
a) vente ou location, ou exposition commerciale;
b) distribution dans un but commercial ou non;
c) communication au public par télécommunication;
d) exécution ou représentation en public.

FEDERAL COURT

NAMES OF COUNSEL AND SOLICITORS OF RECORD

DOCKET:	T-292-04
STYLE OF CAUSE:	BMG CANADA INC., EMI MUSIC CANADA, A DIVISION OF EMI GROUP CANADA INC., SONY MUSIC ENTERTAINMENT (CANADA) INC., UNIVERSAL MUSIC CANADA INC., WARNER MUSIC CANADA LTD., BMG MUSIC, ARISTA RECORDS, INC., ZOMBA RECORDING CORPORATION, EMI MUSIC SWEDEN AB, CAPITOL RECORDS, INC., CHRYSALIS RECORDS LIMITED, VIRGIN RECORDS LIMITED, SONY MUSIC ENTERTAINMENT INC., SONY MUSIC ENTERTAINMENT (UK) INC., UMG RECORDINGS, INC., MERCURY RECORDS LIMITED AND WEA INTERNATIONAL INC. - and - JOHN DOE, JANE DOE AND ALL THOSE PERSONS WHO ARE INFRINGING COPYRIGHT IN THE PLAINTIFFS' SOUND RECORDINGS
PLACE OF HEARING:	TORONTO and OTTAWA, ONTARIO
DATE OF HEARING:	MARCH 12 and 15, 2004
REASONS FOR ORDER AND ORDER :	von FINCKENSTEIN J.

DATED: MARCH 31, 2004

APPEARANCES:

Ronald Dimock Dennis Sloan Bruce Stratton	FOR PLAINTIFF
David van der Woerd	FOR INTERVENER, Electronic Frontier Canada
Phillippa Lawson Howard Knopf Alex Cameron	FOR INTERVENER, Canadian Internet Policy and Public Interest Clinic
James Hodgson Kathryn Podrebarac	FOR NON-PARTY RESPONDENT, Bell Canada
Pat Flaherty Laura Malloni	FOR NON-PARTY RESPONDENT, Rogers Cable
Charles Scott Rocco Di Pucchio	FOR NON-PARTY RESPONDENT, Shaw Communications
Joel Watson	FOR NON-PARTY RESPONDENT, Telus Communications
Robert Bafaro	FOR RESPONDENT

SOLICITORS OF RECORD:

Dimock Stratton Clarizio LLP Toronto, Ontario	FOR PLAINTIFFS
Ross & McBride LLP Hamilton, Ontario	FOR INTERVENER Electronic Frontier Canada
CIPPIC Ottawa, Ontario	FOR INTERVENER Canadian Internet Policy and Public Interest Clinic (CIPPIC)