Court File No. T-292-04

FEDERAL COURT - TRIAL DIVISION

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

WRITTEN REPRESENTATIONS OF SHAW COMMUNICATIONS INC. (Motion Returnable March 12, 2004)

PART I – OVERVIEW OF THE MOTION

1. In this motion brought under Rule 233 of the *Federal Court Rules*, the plaintiff music companies are seeking to compel Shaw Communications Inc ("Shaw"), a "non-party respondent", to disclose certain personal information about certain of its account holders, as specified in the draft Order set out in Schedule "A" to the Notice of Motion.

> Notice of Motion, February 10, 2004, Plaintiff's Motion Record (Shaw), Tab 1

2. This is a precedent-setting motion, which involves the balancing of privacy rights of individuals against the need for disclosure by plaintiffs who wish to pursue civil actions. There has been no prior judicial ruling that has fully and completely considered this issue, and determined the appropriate test to apply.

3. Shaw's position is as follows:

(a) Shaw opposes the motion brought against it;

(b) The affidavits filed and relied upon by the plaintiffs are inadmissible as regarding the pertinent and necessary evidence upon which to base these motions, since they are clearly not sworn on the basis of personal knowledge but on information derived from other unidentified persons, offending rule 81(1)

(c) The affidavit evidence filed by Shaw demonstrates that Shaw cannot answer the questions posed or provide the information sought in the draft Order, with any sufficient degree of certainty;

(d) The information sought by the plaintiffs is intended for use not in the present action (which action may well offend the Court's joinder rules (Rules 101 to 104)), but in some other actions or applications to be commenced by the plaintiffs and it:

a) offends the "implied undertaking" rule;

b) seeks the disclosure of more than "any document that is in the possession of a person who is not a party to the action", as required by Rule 233(1);

c) does not conform with the requirements of Rule 233 since it seeks more than production of a document whose "production could be compelled at trial [in the action]."; and

d) therefore amounts to a request for the issuance of a "civil search warrant" in circumstances where no such warrant is authorized by statute, the Rules of this Court or the common law and in circumstances where no protections for the real targets of the inquiry are offered.

(e) Given the substantial privacy interests at stake which are exemplified by federal statutes that preclude the release of such personal information except in unusual cases, the Court must apply a high threshold test prior to ordering disclosure of the information sought. Here, the plaintiffs have not presented evidence to the Court that establishes a *prima facie* case of copyright infringement on the facts and on the law by anyone, and the motion ought to be dismissed on that basis as well;

(f) In any event, the proposed draft Order:

(i) is too broad in requiring Shaw to disclose personal information and create affidavits, in a manner and to an extent not contemplated by Rule 233 or the other rules;

(ii) makes no provision for the payment of Shaw's costs of this motion or of any discovery of Shaw under Rules 238 and 239; and

(iii) makes no provision for the payment of Shaw's operational and other costs of locating, isolating, vetting and producing any information or documents under Rule 239.

PART II – THE FACTS

Millin Affidavit Inadmissible

4. It is submitted that paragraphs 13 through 92 of the Millin affidavit are inadmissible and should be ignored by the Court. They are based not on personal knowledge, but, apparently on information obtained from some unidentified persons. As such the evidence offends rule 81(1) and the "best evidence" rule and must be disregarded. Mr. Millin made it clear on his cross-examination that his role in the MediaSentry company was "general oversight for the business and [in] particular strategy". MediaSentry has both technical and operations employees who develop programs and monitor the programs that are run, respectively. They do the "hands-on" work. They report through managers to Mr. Millin and other executives. He did not collect the data set out in his affidavit about the alleged infringers. He was not even in the office when the information supposedly reported in his affidavit about, for instance, "Geekboy@KaZaA" (Millin paragraphs 17-25) and "Amanda@KaZaA" (Millin affidavit paragraphs 26-334) was collected. He did not send out any of the 694,000 instant messages referred to in paragraph 13 of his affidavit and did not know to what areas in Canada they were sent.

Millin cross-examination, QQ 34,42-45, 47-48, 109-115, 169-170, 174-177, 240-243

5. The facts upon which Shaw substantially relies are set out in the affidavit of Greg Pultz, Vice President of Internet Systems of Shaw Communications Inc., the officer of Shaw who has overall responsibility for the division that provides all Internet services to Shaw's customers. The facts set out in paragraphs 6 to 35, below, are taken from the Pultz affidavit.

6. At the present time there are over 900,000 subscribers to Shaw's Internet services in B.C. Alberta, Saskatchewan, Manitoba and parts of Northern Ontario.

Affidavit of Greg Pultz ("Pultz"), sworn February 13, 2004 ("Pultz"), Shaw's Preliminary Motion Record Tab 1, p. 1, ff.

7. Further evidence was obtained from the cross-examination of Gary Millin, whose affidavit was filed by the plaintiffs.

Affidavit of Gary Millin, Plaintiffs Motion Record (Shaw) Tab 2

Cross-examination of Gary Millin ("Millin Cross-examination"), March 4, 2004, Shaw's Supplementary Motion Record, Tab 2

Shaw's Business

8. In the areas in which it does business, Shaw provides services as an Internet Service Provider (ISP) to customers. An ISP is the communications facility that typically enables individuals and businesses to connect to the Internet. These services are provided by Shaw through High-Speed connections, which are connected to an internet device through a cable which typically also provides cable TV services.

Shaw's ISP Privacy Policy

9. Shaw usually enters into individual contracts which are made between Shaw and its customers when the customers sign up for Internet services.

10. Shaw's services are provided pursuant to certain policies which are posted for viewing on Shaw's Internet web-site.

11. These policies are referred to as "Terms of Use". Shaw has a Terms of Use policy entitled "Shaw's Customer Privacy Policy", dated April 15, 2002[1]. The second paragraph states the following:

> "Customer privacy is a high priority at Shaw as we have always maintained a policy of protecting our customers' personal information."

It is this publicly stated commitment to protecting the privacy of Shaw's customers' personal information that in large measure dictates Shaw's response to this motion. Shaw believes in this policy.

12. Shaw's Customer Privacy Policy also sets out the various principles and operating details of those principles. The intent of adopting these principles was to effectively mirror and conform to the principles and polices articulated in the *Personal Information Protection and Electronic Documents Act* S.C. 2000, Ch. 5 (PIPEDA)[2]. Shaw became subject to PIPEDA's requirements and obligations on January 1, 2001. Shaw seeks to protect its customers' personal information in accordance with the principles of PIPEDA.

---

[1] Exhibit "A" to the *Pultz* Affidavit, Shaw's Preliminary Motion Record, Tab 1..
[2] Shaw's Preliminary Motion Record, Tab 4.

Shaw's Inability to Provide the Information and Documents sought in this Motion

Pseudonyms

13. The "Peer-to-Peer Network Pseudonyms" referred to in Schedule "A" to the Notice of Motion are entirely meaningless to Shaw. Shaw does not recognize or have any records that could identify any subscriber or account based on that listing of pseudonyms.

IP Addresses and Shaw's Ability to Respond to the Draft Order

14. Although the IP Addresses noted in that column of Schedule "A" to the Notice of Motion are all IP Addresses that are within the blocks of IP Addresses that are assigned to Shaw by the American Registry for Internet Numbers, the international organization that allocates IP Addresses, Shaw cannot with certainty identify from its records the persons who were using the specified IP Addresses on the specified dates and at the specified times.

15. Electronic devices such as personal computers (PCs) and other devices connect to the Internet through a series of industry standards or protocols. The successful operation of these protocols on a world-wide basis requires that certain standards be adhered to by those seeking to communicate over the Internet, and that the equipment that they use for that communication also adheres to certain standards and have certain standardized features.

16. In order for a PC to connect to the Internet, it must be equipped with a device (typically, a network interface card (NIC)) that intermediates electronic signals between the computer and the Internet or another Internet-capable device. A NIC may be a computer "card" that is installed in a "slot" in the PC by the customer (which can then be changed by the customer) or a manufacturer may build it into the PC. Another such Internet-capable device might be a "router" (a device which connects sub-networks together, thereby allowing very large networks to be broken down into more manageable sub-networks), or a device which translates computer signals into communication signals that can be transmitted over co-axial or other types of cable (a "cable modem") in a form that can be understood by another PC or internet device.

17. In order for one of these various devices to connect to the Internet, it must have an identifiable and unique "name" or code which identifies it as the device to or from which information is being sent or received, as the case may be. Such codes are governed by a standard network protocol developed by The Institute of Electrical and Electronics Engineers (IEEE) that is known as the "Ethernet" or the "Fast Ethernet" protocol. Each Ethernet networking device is therefore manufactured and encoded with a unique identifier, the Media Access Control (MAC) Address, by the manufacturer. The unique MAC Address allows the network to identify that individual device at the hardware level.

18. To allow information to be sent across the Internet in blocks or "packets" of data that are manageable by the network, each device communicating on the Internet is also assigned an Internet Protocol (IP) Address. An IP Address is a 32-bit number that identifies the systems that are the source and destination of each packet of information travelling over the Internet. There are several methods or internet "protocols" for managing the transmission of data.

Shaw's Dynamic IP Address System

19. The number of IP Addresses used by Shaw in any area is governed by the number of Shaw subscribers in that area.

20. In the typical case on the Shaw system, when a computer system seeks to send or receive data through the Internet, Shaw's electronic Internet management system assigns an IP Address to the hardware device that it recognizes. This connection is made through a cable modem which is installed in the customer's residence or place of business and is attached to a co-axial cable that is attached to Shaw's cable network.

21. Once the system identifies that the connection is being made through a Shaw cable modem, the Shaw system identifies the MAC Address of the device (usually the NIC in the customer's PC or the router through which the customer's PC is attached to the cable modem) that is so connected and assigns to it an IP Address.

22. Shaw uses an implementation of the Dynamic Host Configuration Protocol (DHCP) to centrally manage and assign IP Addresses throughout its network and for all devices attached to its system. As the name implies, this allocation system is "dynamic", meaning that the IP Addresses which it assigns are typically changeable, depending on circumstances, and are not fixed, permanent or "static". Since, each PC or other device attached through Shaw's system to the Internet needs a unique IP Address, Shaw's DHCP assigns IP Addresses automatically as those machines are connected to the Shaw system. When the device to which an IP Address has been assigned is disconnected from the Shaw system (or for other reasons), the IP Address may be re-assigned to another device which is totally unconnected to the device to which the IP Address in question was originally assigned.

23. Shaw's system maintains logs of when a particular IP Address is assigned to a particular MAC Address (i.e. to a particular electronic device having a particular Ethernet identity). Backups are made of these logs from time to time and these back-ups are saved on a periodic basis. However, the Shaw system does not store or record either the cable modem serial number though which the connection was made, the customer account through which the cable modem connection is billed or the identity of the person who actually caused the device to access the Internet through Shaw's system at the time that the IP Address was assigned, which may have been some time before the time for which connection information is sought.

24. When an Internet device is connected through a Shaw cable modem, it is assigned an IP Address. That IP Address is typically assigned (or "leased") initially for a period of 2 days. When the device is shut down or otherwise disconnected from the Internet, the IP Address that was assigned to it may be reassigned to another device. If the Internet device in question is reconnected from the same general geographic location within a relatively short period of time, the Shaw system may assign the same IP Address to that specific Internet device, but that cannot be assured as that IP Address may, in the meantime, have been assigned to another device used by another subscriber.

25. The use of this implementation of the DHCP system allows more Internet devices to be connected easily and flexibly through the Shaw system in any one area (although not all at the same time) than would be the case if every device was assigned its own static IP Address.

26. A different IP address may also be assigned to the same subscriber account if the user connects a different Internet device (such as a new NIC or router) or for other reasons.

What Shaw's System Can and Cannot Reveal

27. The Shaw system can disclose which IP Address is assigned to which Internet device at the time of inquiry, but that information is not stored on a permanent or historical basis. Thus, Shaw cannot determine from its historical logs what subscriber was using what IP address on a date in the past.

28. Even if Shaw were able to identify with any precision an account to which an IP Address was associated in the past, there is no way that Shaw can identify what person or user was actually using the device and connecting to the Internet or granting access to that device to others through the Internet.

29. Moreover, even if Shaw can determine what subscriber is using an Internet device with a specific MAC Address that is currently connected to its system, that does not with certainty prove that the same device was in use by the same subscriber in the past. Shaw's IP system does not require Shaw's High Speed subscribers to login or otherwise identify themselves. The Shaw system does not use the MAC Address to verify that the person accessing the Internet through the Shaw system is a subscriber to Shaw's Internet services.

30. When a customer changes Internet devices (by installing a new NIC or installing a new router or firewall device), the IP Address dynamically assigned to the customer will change and the former IP Address is no longer with certainty from Shaw's records identifiable or referable to any particular account or customer, on an historical basis.

31. Even if Shaw were to make available records which show what MAC Address is currently assigned to a particular IP Address, and which also shows what IP Address or IP Addresses were assigned to the same MAC Address at some time or date in the past (even within some period of days or hours in the past), Shaw would not be able to provide sworn evidence

that the account currently associated with the MAC address that is using a current IP Address is the same account that was associated with that IP Address in the past.

32. Similarly, if the MAC Address of a device used by a particular user has changed between the past date under inquiry and the current date when an inquiry is made, then there is no way from the Shaw records to even speculate as to the identity of the current user of any IP Address with an IP Address that is associated with some activity in the past.

Conclusion

33. From Shaw's business records, it cannot be determined, to the degree required in a sworn statement, which Shaw subscriber account was assigned the dynamic IP Addresses referred to in the Notice of Motion on the days and at the times noted in those materials. Shaw cannot, therefore, to the degree of certainty required, provide the personal information sought about the 8 IP Addresses noted in the Notice of Motion.

34. Moreover, if Shaw were asked to speculate or required to guess at this type of conclusion about the identity of users or subscribers, Shaw is concerned that it would be required to assume a liability for incorrect information. Shaw might well find itself having to respond to a financial or other type of claim or to a complaint under PIPEDA by a subscriber if the conclusions or guesses were incorrect.

35. If, after a consideration of all the appropriate legal, statutory and other interests, this Court determines that Shaw is required to produce specific business records that it has maintained, it will, of course, do so. But Shaw is not capable of answering the conclusory questions posed in the draft Order.

36. Much of the evidence given by Mr. Pultz of Shaw was confirmed by the plaintiffs' own deponent, Gary Millin of MediaSentry.

37. Mr. Millin was not in a position to dispute any of the technical evidence given by Mr. Pultz.

38. In cross-examination, Mr. Millin confirmed that merely knowing an IP address does not identify a "user". Moreover, Mr. Millin confirmed that while an IP address might identify a computer with a MAC Address, it might only identify a router with a MAC Address, and not the several (up to a hundred or more) devices such as computers, each with their own MAC Addresses, operating behind the router.

Millin cross-examination; Q's. 116, 128-136 and 153-155, pp. 36, 39 and 44-45

39. He acknowledged that a wireless router could be accessed in certain circumstances by anyone with a wireless computer or a wireless adapter, even someone in another house or another office and that externally all such users would appear to be using the same IP Address.

Millin cross-examination; Q's. 147-155, pp. 43-45

40. Further, even though Mr. Millin deposed in his affidavit sworn February 6, 2004 that the ISP's disclosure of identities connected to the list of IP addresses in issue should be "a relatively straightforward task" (para. 93), it is clear that this conclusory statement was simply an assumption on Mr. Millin's part, and was not based upon any personal knowledge of Shaw's systems and databases. In particular, Mr. Millin gave the following evidence on cross-examination:

> 162. Q. This statement in 93 doesn't take account of the problems of static or dynamic IP addresses; it doesn't take account of wireless routers; it doesn't take account of people using a router being behind a router; it doesn't take account of any of those things we've been discussing for the last few minutes, does it?
>
> A. It takes account of it in the fact that we know the IP address that we saw that content coming from, but we can't tell you the user that was at that IP address. And to the extent that someone is using a wireless router and they chose --
>
> 163. Q. Or as in a university, a cyber cafe or in the next building, next office; your statement here doesn't take account of any of those circumstances?
>
> A. All we can see is the IP address that that content is coming from, and it -- it would depend on how a person set up a router or a wireless device to give it public access or not. If they had multiple people using that IP address is something that we can't tell. We see just the IP address that the content is coming from.

164. Q. Right. And when you say it should be relatively straightforward for an ISP to be able to do so, you're not dealing with the circumstances that we've been discussing in the last few minutes when the ISP doesn't know any more than you do about who is using the computer behind the router or who is next door or who is at the cyber cafe or any of that stuff?

A. When I say it should be relatively easy, I would be referring to for the ISP to determine whose account was being used to deliver the content.

165. Q. I see. Assuming that it had a record of the ISP that was assigned to a particular account at that time, but it would be more difficult in the case of a dynamic allocation for ISP, wouldn't it?

A. I made the statement because I would assume that ISPs keep track of, in some kind of log, users that are connected and the date and the time and the IP addresses for a variety of reasons.

166. Q. When you say "users," do you mean the account holders?

A. The account holders.

167. Q. You don't mean the person actually operating the computer?

A. Correct. The account holder.

168. Q. You're assuming that there are logs kept; you don't know that that's the case?

A. Correct.

Millin cross-examination QQ. 164-168, pp. 47-48

MediaDecoy

41. Part of the MediaSentry service include MediaDecoy, which is a program to distribute bogus or inoperative files over the internet, so that persons download them thinking incorrectly that they are music files. The files are made to look like real music files, but they are inoperative. He said at page 34:

A. The intent of MediaDecoy is to minimize
13 the harmful impact of unauthorized files being offered.
14 And so you make a file that looks like the real file, and
15 to the extent people are searching for the illegitimate
16 copies that other people are distributing, we make the
17 non-real file available so that when people get a screen
18 shot of results, they cannot differentiate from the people
19 illegally or distributing the illegitimate content and our
20 content, which appears in the same screen as the other
21 people distributing their files.
22 108. Q. And so the only way to tell them apart
23 is to listen to them?

24 A. That's right.

42. When he was asked to advise, therefore, whether he could tell whether any of the files allegedly copied from the alleged infringers were MediaDecoy files, he said that he did not listen 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

43. Millin also testified that from the file lists attached to his affidavit, one cannot tell

(a) whether the files listed really do contain the musical piece suggested by the title (Q. 212-215

(b) whether the files came from a CD, over the Internet or is a MediaDecoy file (QQ. 209-211)

No Evidence of File Copying other than by MediaSentry

44. Mr. Millin was unable to say whether any files had been copied from Geekboy@KaZaA, other than by Media Sentry.

Millin cross-examination, Q 197

How KaZaA Operates

45. Mr Millin gave evidence about the KaZaA software as follows:

(a) from the main screen, a user cannot "see" that transfers of his or her files are taking place from the user's computer (QQ. 200-202);

(b) for many of the KaZaA software packages, the default condition is that file transfers are permitted and that this feature must be specifically turned off to prevent transfers from the user's computer (QQ 203-204);

(c) files available for transfer from a user of KaZaA can come from a CD or the internet (Q205-211);

(d) even when a user thinks he or she has shut down KaZaA, the program may still be "running" on the user's computer and allowing other to copy files (216-219)

The Plaintiffs' and CRIA's approach to Obtaining Personal Information

46. The Recoding Industry Association of America ("RIAA") is the American counterpart to the Canadian Recording Industry Association ("CRIA"), whose Anti-Piracy Coordinator, Kathy Yonekura, swore one of the affidavits herein on February 10, 2004.

47. Materials published by RIAA[3] deal with the evolution of the RIAA's policy of using subpoenas under American legislation to obtain the names of people they believe are copyright infringers, the problems of following that course of conduct after the *Verizon* case in the United States and the use of other techniques to get around this problem. It appears that the approach proposed to be used by the CRIA in this case is very similar to the approach used by RIAA before the *Verizon* decision - namely to obtain information through a court process and then use that information to seek to "settle" with the alleged infringers or to sue them.

Shaw's Expenses

48. If ordered by the Court to produce specific business records, Shaw's managers and employees will be put to considerable effort and time to collect and verify the documentary information requested concerning the 8 specific IP Addresses set out in the Notice of Motion.

49. In cross-examination (Page 62), Mr. Pultz said the following:

```
Q.   And you talk about considerable effort and time to
  3   collect and verify the documentary information requested.
  4   A.   Yes.
  5   Q.   All right.  Is there more in terms of going through the
  6   process that we discussed and looking at what back-ups might
  7   exist at the server site and the back-ups that might also
  8   exist at the CMTS site that is the -- so we talked about
  9   logs being at the DHCP server site and the CMTS site and
 10   then also at the billing site.  Are there more records that
```

[3] See Exhibits "B" and "C" to the Pultz Affidavit, Shaw's Preliminary Motion Record, Tab 1.

need to be interrogated than what we have gone through there? Is there anything else that you have in mind when you talk about the effort and time to collect and verify the information requested?
A. I don't think we could answer that until we started the investigation.
Q. All right. So you don't today know what time and effort is involved?
A. Today, no.
Q. All right. And -- all right.
A. Other than *it's a lot of work based on what we've talked about. It's a horrendous amount of information that we would have to purge through to find this specific information. If it's available.* (emphasis added)

50. Shaw will also incur, as it has already incurred, considerable legal expenses, both internally and for external counsel, to ensure that the information it can disclose is information that it may disclose, having regard to its statutory obligations under PIPEDA. This is crucial, as Shaw must be certain that it is disclosing only what is required by Court Order, in order to avoid liability under that statute, other statutes in the provinces involved, its contracts and its Terms of Use.

Pultz affidavit. para 40, Shaw's preliminary Motion Record Tab 1

51. This issue of the attempt to identify specific Internet subscribers is of great concern to Shaw, not only as regards this specific case but also for the future. If the relief sought in this case is granted, Shaw is concerned that it will be the subject of many more requests for similar types of information from many different directions, each of which will be a very costly process for Shaw.

PART III – THE LAW

The Fundamental Right to Privacy and Relevant Legislation

52. In modern society, retention of information about oneself is extremely important. Individuals go about their daily lives with the reasonable expectation that personal information about them will remain confidential unless they choose to disclose it. The Supreme Court of

Canada has recognized that "privacy is essential for the well-being of the individual" and, for this reason, it is worthy of constitutional protection.

> *R. v. Dyment*, [1988] 2 S.C.R. 417 at 428; Brief of Authorities of the intervenor CIPPIC, Tab 3.

53. In recognition of this fact, Parliament has recently enacted legislation that speaks to an individual's right to control the collection, use and disclosure of their personal information by organizations in the course of commercial activities. Comparable legislation has also been enacted in several of the Provinces (Quebec, British Columbia and Alberta).

> *Personal Information Protection and Electronic Documents Act,* S.C. 2000, c.5; Preliminary Shaw Motion Record., Tab 4

54. As stated above, Shaw became subject to PIPEDA on January 1, 2001.

55. Disclosure by Shaw of information relating to "personal information" such as names, address, telephone numbers, etc. of its customers is, in the absence of legal justification, a breach of Shaw's obligations under PIPEDA[4] and could subject Shaw to legal sanctions at the hands of its customers or of the regulatory authority (the Federal Privacy Commissioner, etc.).

56. While PIPEDA provides certain bases for disclosure of "personal information"[5], it should be noted that there is no provision in PIPEDA for making such an order on an *ex parte* basis vis-à-vis the person whose personal information is sought.

57. Shaw submits that there is a significant issue whether the PIPEDA legislation contemplates that a civil search warrant should be allowed to override the clear statutory intent of protecting personal information. The following questions arise:

(a) must the inquiry process, that the Plaintiffs seek to invoke, be used in the case in which the order is made?

---

[4] *Personal Information Protection and Electronic Documents Act,* S.C. 2000, Ch. 5, see Shaw's preliminary Motion Record, Tab 4.

[5] See, for example, Principle 4.5 and s. 7(3)(c) and 7(3)(i)

(b) can it be used in another case not yet started?

(c) can it be used to start "settlement" negotiations with an identified person?

58. None of these issues have yet been addressed by a Court. Shaw submits that it would be antithetical to the underlying purpose of the PIPEDA to permit a party to have access to an individual's personal information for the purpose of conducting a "fishing expedition", or for engaging an individual in settlement discussions, which appears to be what the plaintiff music companies are hoping to do here.

The Discovery Rules

59. The present motion purports to be brought under Rule 233. In these circumstances, the plaintiffs seek to use Rule 233 on an *ex parte* basis, without notice to the parties whose personal information is being sought.

60. Rule 233 is limited in scope. It permits an order for production of any *document* (not analysis or deductions or inferences and not a non-party's affidavit verifying certain speculations or conclusions about the actions of the non-party's customers) that is in the possession of a non-party if "…its production could be compelled <u>at trial.</u>"

61. It is submitted that the reference to "at trial" implies that the document will be used in the case in which the motion is brought; not in the trial of other possible actions or proceedings. In this case, there is no contemplation that the document produced under Rule 233 will be used at a trial in this action.

62. The request for an affidavit from the non-party is akin to a demand for "written discovery" from that non-party. It is tantamount to a motion under Rule 238 for an examination of a non-party. However, the same conclusion as set out above for Rule 233 would be reached if the plaintiffs sought a third-party discovery under Rule 238.

63. The language of Rule 238 is consistent with the interpretation of Rule 233, as submitted above. Rule 238(1) permits, under certain circumstances, a "party to an action" to seek discovery from a person who is "not a party to the action … who might have information on an

issue *in the action*." It is submitted that this means in the pending action, not some other action(s) or proceeding(s).

64. Moreover, the process under Rule 238(1) could only be used in certain circumstance. It requires that:

(a) notice to be given to other parties to the action in the action (R. 238(2));

(b) the court may only order third party discovery where, *inter alia*:

(i) it would be unfair not to allow the party an opportunity to question the person before trial (R. 238(3)(c)); and

(ii) the questioning will not cause inconvenience or expense to the other parties (R. 238(3)(d)).

65. It is therefore submitted that the proposed procedure is an abuse of the third party discovery process permitted by Rule 233 (or Rule 238). If permitted, the production/discovery process would be used for a "fishing expedition", which is not allowed on such a discovery.

> *Crestbrook Forest Industries v. Canada (MNR)* [1993] 3 FC 251 (leave to appeal to SCC refused), see at paras. 36 ff. (Shaw's Preliminary Motion Record, Tab 5 (only headnote and paras. 1 and 32-50 reproduced))

66. The cases relied upon by the Plaintiffs in the Motion Record at Tans 6 to 10, from which suggest that other courts have granted orders in the nature sought here, are of little use to support the Plaintiffs' position. They mostly relate to cases which proceeded *ex parte* or where there was no one opposing the order made.

The Plaintiffs Really Seek a Civil Search Warrant

67. It is clear that the Order sought is in the nature of a "civil search warrant" rather than production of documents or discovery in an action or proceeding. Although the present proceeding is couched in terms of "discovery" in an action, clearly this is not, in substance, what is being sought.

68. Paragraph 2(j) of the Notice of Motion specifically states that:

> "the Plaintiffs intend to bring separate applications or actions against each of the Infringers [*sic*] and thus, given the implied undertaking rule and applicable privacy laws, seek leave to use information and documents disclosed pursuant to this Order in all proceedings against the Infringers [*sic*];"

69. It is therefore clear that the information sought in this motion in this action is not information which the plaintiffs intend to use in this action; the applicants are seeking information in this action for use in another *possible* action,

70. The plaintiffs seek exemption from the "implied undertaking", so that they can transfer information from this action to one or more other contemplated actions (draft Order paragraph 3)

71. The plaintiffs are clearly not intending to proceed with this action, once the information is obtained. Rather, they may be starting other actions against the persons identified, but other materials (US statements and press releases) suggest that they really want to use the information not specifically to start another action but really to engage in "settlement discussions" with the persons sought to be identified.

The Plaintiffs have not met the threshold test

72. Even apart from the above, Shaw submits that, where there is another competing interest at stake – such as the recognized privacy interests in this case – the Court should apply a higher threshold prior to making an order pursuant to Rule 233.

73. In this respect, Shaw notes and relies upon the submissions that have been made to the Court by the Canadian Internet Policy and Public Interest Clinic ("CIPPIC") at paragraphs 22 to 37 of its Written Representations. In particular, Shaw submits that the plaintiffs' attempted use of Rule 233 in these circumstances is akin to a motion for an *Anton Pillar* order, and the Court should therefore apply a similar test (i.e., a strong *prima facie* case) prior to ordering disclosure. Indeed, in many respects this proceeding is even more invasive than an *Anton Pillar* application, where there are very strict rules for the protection of the target, the relief is sought in the very action, an action in which the "target" is also a party and has an opportunity to seek relief from the Court relating both to the execution of the "search warrant" and the use to which seized

material may be made. None of this can be said for the present case, in which the "targets" are not even before the Court.

74. Having regard to the factors set out in paragraph 37 of CIPPIC's Written Representations, Shaw submits that the plaintiffs are not entitled to the relief sought. In particular, based on the record presently before the Court, the plaintiffs have come woefully short of establishing a strong *prima facie* case of copyright infringement against the John and Jane Doe defendants.

75. Although the plaintiff music companies have stated a claim for, *inter alia*, a declaration that they are the owners of copyright in the various sound recordings listed in Schedule A to the Statement of Claim, and that those copyrights have been infringed by the John and Jane Doe defendants, they have presented no direct evidence of copyright ownership or of infringement, preferring instead to rely almost exclusively upon hearsay and conjecture.

76. While Shaw certainly adopts the arguments made by CIPPIC with respect to the legality of the activity taking place in this case via the Kazaa peer-to-peer service, it is abundantly clear that the evidence relied upon by the plaintiffs does not meet the threshold test in any event. For example, the Affidavits relied upon by the plaintiffs are, to a very large extent, not based on any personal knowledge whatsoever. Thus, for example:

(a) Mr. Millin himself has not listened to any of the files that were downloaded from the Internet by MediaSentry in order to confirm that the files that were downloaded correspond to files in which the plaintiffs claim to own copyright (see questions 189 to 195 at pages 52 to 53 of Mr. Millin's cross examination). On this point, Mr. Millin confirmed on cross-examination that anybody can give any file name that they want to a file, so that the name alone does not necessarily correspond to the contents of the file. As well, as part of the services it offers, MediaSentry itself floods the internet with so-called "dummy" files, being files that are meant to look exactly like a particular music file, but which contain nothing when downloaded and opened (see QQ. 104-108, p. 33). Mr. Millin therefore cannot even testify from personal knowledge that the files that his company downloaded were not "dummy" files or files simply shared the

same name as music recordings in which the plaintiffs claim to own copyright. Ms. Yonekura, who is the Anti-Piracy Co-ordinator for CRIA, similarly did not attest to having listened to any of the files that were downloaded. Simply put, there is no evidence before the Court that any material that infringed copyright was downloaded from any of the John and Jane Doe defendants.

(b) Mr. Millin had no knowledge of whether the files contained in the shared directories of the John and Jane Doe's in this case have been downloaded by anyone other than MediaSentry itself (see Q. 197, p. 54).

77. In addition to the above, Mr. Millin also admitted on cross-examination that a Kazaa user might believe that he/she had shut down the software, but the software might still be running in the user's system tray, without the user's knowledge. This, coupled with the fact that the Kazaa software by default is set to allow sharing of files and does not, on the main screen, advise the user that an upload is taking place, makes it quite probable that a user of Kazaa might not be aware that he/she was potentially engaging in any activity that infringes copyright simply by installing and opening the software.

Transcript of the cross-examination of Gary Millin taken on March 4, 2004; QQ. 200-204, pp. 54-55.

78. The plaintiffs bear the burden on this motion of presenting evidence to the Court of a strong prima facie case. For the reasons expressed above, they have failed to meet this burden. The Court ought not to allow the clear privacy rights of the John and Jane Doe defendants to be trumped in this case on the basis of the weak record presented by the plaintiffs, who have had ample time and certainly have ample resources to have done so.

Shaw's Costs and Expenses

79. If finally ordered by the Court to produce specific business records, Shaw's managers and employees will likely be put to considerable effort and time to collect and verify whatever documentary information it has related to that requested concerning the 8 specific IP Addresses set out in the Notice of Motion. It is to be anticipated that Shaw will also incur, as it has already

incurred, considerable legal expenses, both internally and for external counsel, to ensure that the information we can disclose is information that we may disclose, having regard to our statutory obligations under PIPEDA. This is crucial, as Shaw must be certain that it is disclosing only what is required under a court Order, in order to avoid liability under that statute, other statutes in the provinces involved, its customer contracts and its Terms of Use.

80. In respect of any Order made against Shaw, adequate provisions should be made to cover its costs of this motion, the expenses of its staff and its solicitors in obtaining and reviewing any information sought and all other expenses allowable under rule 239.

ALL OF WHICH IS RESPECTFULLY SUBMITTED this 10th day of March, 2004.

_____

Charles F. Scott
Rocco DiPucchio

LAX O'SULLIVAN SCOTT LLP
Counsel
1920-145 King Street West
Toronto, Ontario M5H 1J8

Solicitors for the Non-Party Respondent
Shaw Communications Inc.