

T-292-04
2004 FC 488

T-292-04
2004 CF 488

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, Capital 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)

v.

John Doe, Jane Doe and All Those Persons Who are Infringing Copyrights in the Plaintiffs' Sound Recordings (Defendants)

INDEXED AS: BMG CANADA INC. v. JOHN DOE (F.C.)

Federal Court, von Finckenstein J.—Toronto and Ottawa, March 12 and 15; Ottawa, March 31, 2004.

Copyright—Infringement—Recording industry businesses seeking order for disclosure by internet service providers (ISPs) of customers' identities—Customers said to be guilty of copyright infringement by trading in music downloaded from internet—Internet users operating under software-related pseudonyms—File-sharing programs utilized—Motion denied—Affidavit in support failing to make out prima facie case—Hearsay—Sworn by President of online anti-privacy protection company when other employees in better position to swear, undergo cross-examination—Affiant never listened to files so no evidence files offered for uploading infringing—No evidence copyright infringed—Copyright is creature of statute, tort concepts inapplicable—Downloading of song for personal use not infringement: Act, s. 80(1)—No evidence alleged infringers distributed, authorized reproduction of sound recordings—Analogy to CCH Canadian Ltd. v. Law Society of Upper Canada wherein S.C.C. held provision of photocopiers does not constitute authorization—No distribution absent positive act by shared directory owner—Exclusive right of making available provided for by World Intellectual Property Organization Performances and Phonograms Treaty but Treaty not yet implemented by Canada—No secondary infringement absent knowledge on infringer's part: Act, s. 27(2)—While plaintiffs have copyright entitled to protection, Court not satisfied as to reliability of

BMG Canada Inc., EMI Music Canada, une division du 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, Capital Records, Inc., Chrysalis Records Limited, Virgin Records Limited, Sony Music Entertainment Inc., Sony Music Entertainment (UK) Inc., UMG Recordings, Inc., Mercury Records Limited et WEA International Inc. (demandeurs)

c.

John Doe, Jane Doe et toutes les personnes qui violent le droit d'auteur des demandeurs dans leurs enregistrements sonores (défendeurs)

RÉPERTORIÉ: BMG CANADA INC. c. JOHN DOE (C.F.)

Cour fédérale, juge von Finckenstein—Toronto et Ottawa, 12 mars et 15 mars; Ottawa, 31 mars 2004.

Droit d'auteur—Violation—Des sociétés membres de l'industrie de l'enregistrement demandent qu'une ordonnance soit délivrée pour obtenir de certains prestataires de service Internet (les PSI) la divulgation de l'identité de certains clients—Elles soutiennent que les clients ont violé la législation sur les droits d'auteur en échangeant des œuvres musicales téléchargées d'Internet—Les utilisateurs d'Internet ont adopté des pseudonymes associés au logiciel qu'ils utilisent—Des logiciels de partage sont utilisés—Requête rejetée—Le contenu de l'affidavit des demandeurs est insuffisant pour établir l'existence d'une preuve convaincante à première vue—Où-dire—Affidavits déposés par le président d'une société qui offre une protection contre le piratage en ligne alors qu'il devait y avoir d'autres employés qui étaient mieux placés pour souscrire les affidavits en cause et pour répondre aux questions des défendeurs en contre-interrogatoire—L'auteur des affidavits n'a écouté aucun des fichiers, par conséquent, il n'existe aucune preuve que les fichiers rendus disponibles pour le téléchargement sont des contrefaçons des fichiers des demandeurs—Aucune preuve de violation du droit d'auteur—La loi concernant le droit d'auteur tire son origine de la loi, les principes de la responsabilité délictuelle ne s'appliquent pas—Télécharger une chanson pour usage privé ne constitue pas une violation du droit: art. 80(1) de la Loi sur le droit d'auteur—Aucune preuve que les violateurs présumés auraient distribué des enregistrements sonores ou

information to be disclosed.

Practice — Discovery — Production of Documents — Federal Court Rules, 1998, rr. 233, 238 application for order requiring production by non-party to action — Identity of customers of internet service providers (ISPs) — Copyright infringement by trading in recorded music downloaded from internet alleged by recording companies — Plaintiffs unable to identify proposed defendants due to use of software-related pseudonyms — Infringers said to utilize file-sharing programs — ISP account holders have expectation identities kept confidential — Unavailability of equitable bill of discovery once action commenced — Relief available only under rr. 233, 238 — Five requirements for relief listed — R. 233 deals with document disclosure, not requiring their creation — No pre-existing documents linking IP address to ISP customer — Motion denied — Plaintiffs' affidavit failing to establish prima facie case — Hearsay by President of online anti-privacy protection business — Grounds for belief insufficiently indicated — Other employees in better position to swear affidavits, undergo cross-examination — Non-compliance with best-evidence rule — President never listened to files, so no evidence files offered for uploading were infringing — No evidence of connection between pseudonyms, IP addresses — No evidence copyright law infringed — Court not told by affidavits ISPs only practical source of names behind pseudonyms — While privacy not to be used as shield against civil, criminal liability, is worthy of constitutional protection, significant for public order — Due to passage of time since information relied upon herein gathered, reliability diminished, innocent account holder might be identified — Privacy interest outweighing public interest favouring disclosure — Had requested order been granted, would have been subject to restrictions to protect defendants' privacy interests.

autorisé leur reproduction — Analogie avec l'arrêt de la Cour suprême du Canada CCH Canadienne Ltée c. Barreau du Haut-Canada dans lequel on a conclu que le fait de mettre sur place des appareils qui permettent de faire des copies ne correspond pas à autoriser la violation du droit d'auteur — Pas de distribution sans un acte positif de la part du propriétaire du répertoire partagé — Le droit exclusif de mettre à disposition est prévu dans le Traité de l'Organisation mondiale de la propriété intellectuelle sur les interprétations et exécutions et les phonogrammes mais ce traité n'a pas encore été ratifié par le Canada — Aucune violation à une étape ultérieure si aucune preuve que le violateur en avait connaissance: art. 27(2) de la Loi sur le droit d'auteur — Bien que les demandeurs aient droit à ce que leur droit d'auteur soit protégé, la Cour n'est pas convaincue que les renseignements qui seraient divulgués sont fiables.

Pratique — Communication de documents et interrogatoire préalable — Production de documents — Requête en vertu des règles 233 et 238 des Règles de la Cour fédérale (1998) en vue d'obtenir une ordonnance enjoignant à un tiers de divulguer l'identité de certains clients de certains prestataires de service Internet (les PSI) — Les sociétés d'enregistrement prétendent qu'il y a eu violation de la législation sur les droits d'auteur occasionnée par l'échange d'œuvres musicales téléchargées d'Internet — Les demandeurs ne peuvent identifier les utilisateurs d'Internet en question puisqu'ils ont adopté des pseudonymes associés au logiciel qu'ils utilisent — On a prétendu que les violateurs utilisent des logiciels de partage de fichiers — Les clients des PSI ont une attente d'anonymat — On ne peut pas se servir de l'interrogatoire préalable en equity une fois que l'action a été introduite — Redressement prévu aux règles 233 et 238 — Énumération des cinq conditions préalables à l'octroi d'un tel redressement — La règle 233 a pour objectif d'ordonner la production de documents et non leur création — Pas de documents faisant le lien entre une adresse IP et un client donné d'un PSI — Requête rejetée — L'affidavit des demandeurs n'établit pas l'existence d'une preuve convaincante à première vue — Oui-dire de la part du président d'une société qui offre une protection contre le piratage en ligne — Il ne dit pas sur quoi il fonde sa conviction — D'autres employés étaient mieux placés pour souscrire les affidavits en cause et pour répondre aux questions des défendeurs en contre-interrogatoire — Non-respect de la règle de la meilleure preuve — Le président n'a jamais écouté aucun des fichiers, par conséquent, il n'existe aucune preuve que les fichiers rendus disponibles pour le téléchargement violent le droit d'auteur — Aucune preuve établissant un lien entre les pseudonymes et les adresses IP — Aucune preuve de violation du droit d'auteur — La Cour ne peut déterminer à partir des affidavits si les PSI sont la seule source pratique pour obtenir l'identité des utilisateurs de pseudonymes — Bien que le droit de chacun à la vie privée ne peut être invoqué par une personne pour échapper à sa responsabilité, civile ou criminelle, il mérite une

protection constitutionnelle, il revêt une importance capitale sur le plan de l'ordre public — Avec le temps qui s'écoule, les renseignements en cause sont plus difficiles à obtenir et leur fiabilité diminue, il existait une possibilité sérieuse que l'on communique l'identité d'un client innocent — Le respect de la vie privée prime l'intérêt public à la divulgation — Si l'ordonnance demandée avait été délivrée, il aurait fallu imposer certaines restrictions afin de protéger le droit à la vie privée des défendeurs.

This was a motion brought by a number of corporations in the recording industry business seeking disclosure by certain internet service providers (ISPs) of the identity of customers said to be guilty of copyright infringement by trading in music downloaded from the internet. Plaintiffs could not identify these internet users because they operate under pseudonyms related to software. Relief was sought under *Federal Court Rules, 1998* rules 233 and 238. Plaintiffs said that each of these unidentified defendants has downloaded in excess of 1000 songs onto home computers. It was said that defendants utilize the KaZaA and iMesh file-sharing programs, which allows them to share computer files with others connected to a peer-to-peer network. They possess software by which they can search the pool of shared files such as by title or artist. Multiple transfers to other users may take place simultaneously from a user's computer.

It was agreed by all parties that internet service provider account holders expect that their identities will be kept confidential. This expectation is based on both sections 3 and 5 of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and on their ISP account agreements. But, under PIPEDA, paragraph 7(3)(c), an ISP may disclose personal information if so required by court order.

While a potential plaintiff may seek pre-action discovery, by way of an equitable bill of discovery, to ascertain a defendant's identity, once an action has been commenced—even by naming as defendants John and Jane Doe—plaintiff must have recourse to rule 233 or 238. But the same principles should apply to a rule 238 application as to an equitable bill of discovery: (1) applicant must establish a *prima facie* case against the unknown alleged wrongdoer; (2) person from whom discovery is sought must be more than an innocent bystander; (3) that person must be only practical information source; (4) said person must be reasonably compensated for expenses of compliance with the discovery order; and (5) the

Il s'agit d'une requête déposée par un certain nombre de sociétés membres de l'industrie de l'enregistrement pour obtenir de certains prestataires de service Internet (les PSI) la divulgation de l'identité de certains clients qu'ils soutiennent avoir violé la législation sur les droits d'auteur en échangeant des œuvres musicales téléchargées d'Internet. Les demandeurs ne peuvent identifier les utilisateurs d'Internet en question, puisqu'ils ont adopté des pseudonymes associés au logiciel qu'ils utilisent. Les demandeurs sollicitent une ordonnance en vertu des règles 233 et 238 des *Règles de la Cour fédérale (1998)*. Les demandeurs soutiennent que les défendeurs ont chacun téléchargé sur leur ordinateur personnel plus de 1 000 chansons. On a prétendu que les défendeurs utilisent les logiciels de partage de fichiers KaZaA et iMesh qui leur permettent de partager des fichiers avec d'autres utilisateurs reliés à un réseau d'homologues. Ils possèdent des logiciels qui leur permettent de faire une recherche dans le réservoir de fichiers partagés en utilisant un titre ou un nom d'artiste. L'ordinateur d'un utilisateur peut servir simultanément à des transferts multiples vers d'autres utilisateurs.

Toutes les parties ont convenu que les clients des PSI ont une attente d'anonymat. Cette attente du respect de leur vie privée se fonde à la fois sur leurs contrats avec les PSI et sur les articles 3 et 5 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). Cependant, l'alinéa 7(3)c) de la LPRPDE porte que les PSI peuvent communiquer des renseignements personnels sans le consentement des intéressés lorsque ces renseignements sont exigés par ordonnance d'un tribunal.

Lorsqu'un demandeur potentiel recherche un interrogatoire préalable afin de connaître l'identité d'un défendeur, il peut avoir recours à l'interrogatoire préalable prévu en *equity*, mais pas lorsqu'une action a déjà été introduite—même si les défendeurs ne sont cités que sous les noms de John et Jane Doe—le demandeur doit s'en remettre à l'application des règles 233 et 238. Les mêmes principes devraient s'appliquer à une demande en vertu de la règle 238 et à un interrogatoire préalable en *equity*: 1) le demandeur doit démontrer qu'il existe à première vue quelque chose à reprocher à l'auteur inconnu du préjudice; 2) la personne devant faire l'objet d'un interrogatoire préalable doit être plus qu'un simple spectateur;

public interests favouring disclosure must outweigh legitimate privacy concerns.

Plaintiffs also attempted to rely on rule 233, but that rule compels the disclosure of documents, not their very creation. In the instant case, there were no pre-existing documents linking an IP address to an ISP customer.

Held, the motion should be denied.

(1) As to a *prima facie* case, the content of plaintiffs' affidavits was deficient. Deposed to by the President of an online anti-privacy protection company, they were based upon information gained from his employees and accordingly consisted of largely hearsay. While hearsay is admissible under subsection 81(1) of the Rules if the grounds for the belief are set forth, these were insufficiently stated herein. There must have been other MediaSentry employees who would have been in a better position to swear the affidavits and undergo cross-examination thereon. No explanation was given for non-compliance with the best-evidence rule. Furthermore, the affiant acknowledged that he had not listened to any of the files copied from the alleged infringers and there was accordingly no evidence before the Court as to whether the files offered for uploading were infringed files of plaintiffs.

A second problem was that there was no evidence of connection between the pseudonyms and the IP addresses. Neither the affidavits nor the cross-examination thereon provided clear evidence as to how the pseudonyms of the KaZaA or iMesh users were linked to the IP addresses identified by MediaSentry. While the affidavit indicated that Geekboy@KaZaA's IP was 24.84.179.98 and that, according to the American Registry for Internet Numbers' public database, that address had been assigned to Shaw Communications (one of the ISPs from which disclosure is sought), no evidence explained how the pseudonym "Geekboy@KaZaA" was linked to the IP address 24.84.179.98 in the first place. It would be irresponsible in these circumstances for the Court to order disclosure of the name of the account holder of IP address 24.84.179.98 thereby exposing that person to litigation.

The next question was whether there was evidence that copyright had been infringed. Plaintiffs say that the alleged

3) la personne doit être la seule source pratique de renseignements; 4) la personne doit recevoir une compensation raisonnable pour les débours occasionnés par son respect de l'ordonnance portant interrogatoire préalable; 5) l'intérêt public à la divulgation doit l'emporter sur l'attente légitime de respect de la vie privée.

Les demandeurs fondent aussi leur requête sur la règle 233, mais cette disposition a pour objectif d'ordonner la production de documents et non leur création. En l'espèce, il n'existe pas de documents faisant le lien entre une adresse IP et un client donné d'un PSI.

Jugement: la requête est rejetée.

1) En ce qui concerne la prétention des demandeurs qu'il existe à première vue quelque chose à reprocher à quelqu'un, le contenu des affidavits des demandeurs est insuffisant. Déposés par le président d'une société qui offre une protection contre le piratage en ligne, ils sont fondés sur des renseignements qu'il a obtenus de ses employés et constituent donc en grande partie du ouï-dire. En vertu du paragraphe 81(1) des Règles le ouï-dire est admissible à condition que les motifs à l'appui soient énoncés, or aucun motif n'est énoncé en l'espèce. Il devait y avoir d'autres employés de MediaSentry qui étaient mieux placés pour souscrire les affidavits en cause et pour répondre aux questions des défendeurs en contre-interrogatoire. Aucune explication n'a été donnée concernant le non-respect de la règle de la meilleure preuve. De plus, l'auteur des affidavits a témoigné qu'il n'avait écouté aucun des fichiers copiés par les violeurs présumés et, par conséquent, la Cour n'a été saisie d'aucune preuve que les fichiers rendus disponibles pour le téléchargement sont des contrefaçons des fichiers des demandeurs.

Le deuxième problème c'est qu'il n'y a aucune preuve de lien entre les pseudonymes et les adresses IP. Toutefois, ni les affidavits, ni le contre-interrogatoire n'apportent une preuve claire et détaillée de comment on a établi un lien entre les pseudonymes des utilisateurs de KaZaA ou iMesh et les adresses IP identifiées par MediaSentry. Malgré que l'affidavit mentionnait que l'adresse IP de Geekboy@KaZaA était 24.84.179.98 et que, selon la banque de données publiques de l'American Registry for Internet Numbers, l'adresse a été assignée à Shaw Communications (l'un des PSI duquel on cherche à obtenir divulgation), aucune preuve n'indique comment, au départ, le pseudonyme «Geekboy@KaZaA» a été lié à l'adresse IP 24.84.179.98. Dans ces circonstances, la Cour agirait de façon irresponsable en ordonnant la divulgation du nom du client correspondant à l'adresse IP 24.84.179.98, l'exposant ainsi à une poursuite.

La question suivante consiste à savoir s'il y a une preuve de violation du droit d'auteur. Les demandeurs affirment que les

infringers: installed the peer-to-peer application on their computers; copied files to “shared directories”; used ISP services to connect their computers to the internet; ran the peer-to-peer application while on the internet and made files in the shared directories available for copying, transmission and distribution to any one of millions of users of the peer-to-peer service. It was argued that the *Copyright Act* was thus infringed by this reproduction, authorization of reproduction and distribution of unauthorized copies of sound recordings. Further, there was the possession, for the purpose of distribution, of unauthorized copies which the infringers either knew or should have known were infringing.

Copyright law is a creature of statute and it does not assist the interpretive analysis to import tort concepts. Under Act, subsection 80(1), the downloading of a song for a person’s private use does not constitute infringement. There was here no evidence that the alleged infringers either distributed or authorized the reproduction of sound recordings. All they did was place personal copies into shared directories accessible by other computer users. The judgment of the Supreme Court of Canada in *CCH Canadian Ltd. v. Law Society of Upper Canada* is authority for the proposition that the provision of facilities that allow copying does not amount to authorizing infringement. How is what was done here different from a library placing a photocopier in a room full of copyrighted material? In either case the element of authorization is missing. McLachlin C.J. wrote in her *CCH* opinion that courts “should presume that a person who authorizes an activity does not only so far as it is in accordance with the law”.

Nor is there distribution absent a positive act by the owner of the shared directory, such as sending copies or advertising the material’s availability for copying. While the exclusive right of making available is covered by the *World Intellectual Property Organization Performances and Phonograms Treaty* of 1996, it remains to be implemented by Canada and so forms no part of our law of copyright. Again, secondary infringement had not been made out since knowledge on the infringer’s part, a necessary condition under subsection 27(2) of the *Copyright Act*, was not demonstrated.

(2) This requirement was met in that the internet access providers were not mere bystanders but rather the means by

violateurs présumés ont installé un logiciel de partage des fichiers entre homologues sur leurs ordinateurs, copié des fichiers sur des «répertoires partagés», utilisé les services des PSI pour relier leurs ordinateurs à Internet, fait fonctionner le logiciel de partage des fichiers entre homologues sur leurs ordinateurs alors qu’ils étaient connectés à Internet et ont rendu les fichiers des répertoires partagés disponibles pour leur copie, transmission et distribution à n’importe lequel des millions d’utilisateurs du service de partage des fichiers entre homologues. Les demandeurs prétendent que la *Loi sur le droit d’auteur* a été violée par la reproduction, l’autorisation de reproduire et la mise en circulation de copies non autorisées des enregistrements sonores. De plus, il y a la possession de copies non autorisées que les violateurs présumés savaient, ou devaient savoir, être des contrefaçons, dans le but de les mettre en circulation.

La loi concernant le droit d’auteur tire son origine de la loi et il n’est pas utile, aux fins de l’interprétation législative, d’introduire les principes de la responsabilité délictuelle. Selon le paragraphe 80(1) de la *Loi sur le droit d’auteur*, le fait de télécharger une chanson pour usage privé ne constitue pas une violation du droit d’auteur. On n’a déposé aucune preuve que les violateurs présumés auraient distribué des enregistrements sonores ou autorisé leur reproduction. Ils ont simplement placé leurs propres copies dans les répertoires partagés accessibles à d’autres utilisateurs. L’arrêt de la Cour suprême du Canada *CCH Canadienne Ltée c. Barreau du Haut-Canada* appuie la thèse selon laquelle le fait de mettre sur place des appareils qui permettent de faire des copies ne correspond pas à autoriser la violation du droit d’auteur. Quelle réelle différence existe-t-il entre ce qui a été fait et une bibliothèque qui place une photocopieuse dans une pièce remplie de documents visés par le droit d’auteur? Dans les deux cas il manque l’autorisation. La juge en chef McLachlin a écrit dans l’arrêt *CCH* que les tribunaux «doivent présumer que celui qui autorise une activité ne l’autorise que dans les limites de la légalité».

Il n’y a pas de distribution sans un acte positif de la part du propriétaire du répertoire partagé, comme l’envoi de copies ou le fait d’annoncer qu’elles sont disponibles pour qui veut les copier. Malgré que le droit exclusif de mettre à disposition soit prévu dans le *Traité de l’Organisation mondiale de la propriété intellectuelle sur les interprétations et exécutions et les phonogrammes* de 1996, ce traité n’a pas encore été ratifié par le Canada et il ne fait donc pas partie de la législation canadienne sur le droit d’auteur. Finalement, les demandeurs soutiennent qu’il y a eu violation à une étape ultérieure, contrairement au paragraphe 27(2) de la *Loi sur le droit d’auteur*, mais ils n’ont présenté aucune preuve que le violateur en avait connaissance.

(2) Cette exigence a été satisfaite en ce que les fournisseurs d’accès ne sont pas de simples spectateurs et que c’est par leur

which downloaders and uploaders access the internet and contact one another.

(3) The affidavits filed in support of this motion failed to provide the information which would allow the Court to make a determination as to whether the ISPs were the only practical source of the names behind the pseudonyms.

(4) As to reasonable compensation for expenses, it would not be easy to provide the name and address of an account holder who used a specific IP address at a given time. The point was made in an affidavit filed by Telus that, while it can identify who opened an account, it would be incapable of identifying who was using the computer at the time of the alleged infringement. For example, the account holder could be an institution or there could be a local area network having numerous users.

(5) Turning to a consideration of competing interests, the importance of privacy protection to Canadian society was underlined in the opinion of Lamer J. in the Supreme Court case *R. v. Dymont*: privacy “is worthy of constitutional protection, but it also has profound significance for the public order”. In an Ontario case, *Irwin Toy Ltd. v. Doe*, Wilkins J. wrote that “it is understood that a person’s internet protocol address will not be disclosed” and added that “some degree of privacy or confidentiality” was “in keeping with what should be perceived as being good public policy”. That being said, privacy cannot be used as a shield against civil or criminal liability. Both statute and case law require the Court to balance privacy rights against the rights of other individuals and the public interest. Reference was made to a number of Canadian cases in which courts have ordered third parties to disclose documents identifying the name and address of a defendant previously identified only by an internet protocol address.

Plaintiffs have a legitimate copyright in their works and are entitled to protect it against infringement. But, prior to ordering disclosure, the Court would have to be satisfied that the information to be disclosed was reliable and any order made should include appropriate restrictions and provisions for confidentiality. The evidence herein had been gathered from October to December, 2003 but the notice of motion was filed only in February, 2004. This delay not only rendered the requested information more difficult to obtain but also decreased its reliability. There was a serious possibility that an innocent account holder might be identified. In the result, the privacy interest outweighed the public interest favouring disclosure.

entremise que les personnes qui font du télédownloadement et du téléchargement accèdent à Internet et entrent en contact.

3) Les affidavits déposés à l’appui de la présente requête ne donnent pas les renseignements qui permettraient à la Cour de déterminer si les PSI sont la seule source pratique susceptible de fournir les noms qui correspondent aux pseudonymes.

4) Pour ce qui est de la compensation raisonnable pour les débours, il n’est pas facile de trouver le nom et l’adresse du client qui a utilisé une adresse IP à un moment précis. Telus a fait remarquer, dans un affidavit qu’elle a déposé, que, bien qu’elle puisse dire qui a ouvert un compte, elle n’est pas capable de savoir quelle personne était à l’ordinateur au moment de la prétendue violation. Par exemple, le client peut être une institution ou un réseau local accessible à plusieurs utilisateurs.

5) En ce qui concerne la question des intérêts opposés, l’importance de la protection de la vie privée pour la société canadienne a été soulignée par le juge Lamer dans l’arrêt de la Cour suprême *R. c. Dymont*: la notion de vie privée «mériterait une protection constitutionnelle, mais elle revêt aussi une importance capitale sur le plan de l’ordre public». Dans une cause ontarienne, *Irwin Toy Ltd. c. Doe*, le juge Wilkins a écrit qu’«il est entendu qu’on ne divulgue pas l’adresse IP d’un client» et a ajouté qu’«il y a une sécurité importante rattachée à une certaine garantie de confidentialité» et que «cette réalité respecte aussi ce que l’on peut concevoir comme une bonne politique d’intérêt public». Cela dit, le droit de chacun à la vie privée ne peut être invoqué par une personne pour échapper à sa responsabilité, civile ou criminelle. La loi et la jurisprudence exigent que la Cour recherche un équilibre entre le droit à la vie privée, les droits des tiers et l’intérêt public. On cite certaines décisions canadiennes dans lesquels les cours de justice ont ordonné à des tiers de communiquer des documents contenant les nom et adresse d’un défendeur dont on ne connaissait que l’adresse du protocole d’Internet.

Les demandeurs ont un droit d’auteur légitime sur leurs œuvres et ils ont le droit d’être protégés de toute violation. Toutefois, avant d’ordonner la communication, la Cour doit être convaincue de façon évidente que les renseignements qui seraient divulgués sont fiables et toute ordonnance de cette nature devrait aussi être assortie des restrictions et mesures de confidentialité appropriées. En l’espèce, la preuve a été collectée entre octobre et décembre 2003, mais l’avis de requête n’a été déposé que le 11 février 2004. Ce retard a eu pour conséquence que les renseignements en cause sont plus difficiles à obtenir et que leur fiabilité est réduite. Il existait une possibilité sérieuse que l’on communique l’identité d’un client innocent. Par conséquent, le respect de la vie privée prime l’intérêt public à la divulgation.

Had an order been granted as asked by plaintiffs, it would have been subject to restrictions in order to safeguard the privacy interests of the as yet unnamed defendants. An invasion of privacy should always be as limited as possible. It would also have provided that only the internet pseudonyms appear as defendants in the statement of claim. A confidential annex would have been added to the statement of claim relating each pseudonym to the name and address of an ISP account holder. Finally, the ISPs would not have been required to provide affidavits in support of their findings.

STATUTES AND REGULATIONS JUDICIALLY CONSIDERED

Copyright Act, R.S.C., 1985, c. C-42, ss. 27(2) (as am. by S.C. 1997, c. 24, s. 15), 34(1) (as am. *idem*, s. 20), 37 (as am. *idem*), 80 (as am. *idem*, s. 50).
Federal Court Rules, 1998, SOR/98-106, rr. 41(1), 55, 81, 222, 232, 233, 238.
Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, ss. 3, 4(3), 5, 7(3)(c),(d),(e),(h.2),(i), Sch. 1.

CASES JUDICIALLY CONSIDERED

APPLIED:

Norwich Pharmacal Co. v. Customs and Excise Comrs., [1974] A.C. 133 (H.L.); *Glaxo Wellcome PLC v. M.N.R.*, [1998] 4 F.C. 439; (1998), 162 D.L.R. (4th) 433; 7 Admin. L.R. (3d) 147; 20 C.P.C. (4th) 243; 81 C.P.R. (3d) 372; 228 N.R. 164 (C.A.); *Regina v. Maligne Building Ltd. et al.* (1980), 54 C.P.R. (2d) 11; 37 N.R. 526 (F.C.A.); *R. v. A. & A. Jewellers Limited*, [1978] 1 F.C. 479; [1977] C.T.C. 428 (T.D.); *Compo Company Ltd. v. Blue Crest Music Inc. et al.*, [1980] 1 S.C.R. 357; (1979), 105 D.L.R. (3d) 249; 45 C.P.R. (2d) 1; 29 N.R. 296; *CCH Canadian Ltd. v. Law Society of Upper Canada*, [2004] 1 S.C.R. 339; (2004), 226 D.L.R. (4th) 395; 30 C.P.R. (4th) 1; 317 N.R. 107; *R. v. Dymont*, [1988] 2 S.C.R. 417; (1988), 73 Nfld. & P.E.I.R. 13; 55 D.L.R. (4th) 503; 229 A.P.R. 13; 45 C.C.C. (3d) 244; 66 C.R. (3d) 348; 38 C.R.R. 301; 10 M.V.R. (2d) 1; 89 N.R. 249; *Irwin Toy Ltd. v. Doe* (2000), 12 C.P.C. (5th) 103 (Ont. Sup. Ct.).

CONSIDERED:

MGM Studios, Inc. v. Grokster, Ltd., 259 F. Supp.2d 1029 (C.D. Cal. 2003).

REFERRED TO:

Ontario First Nations Limited Partnership v. John Doe, June 3, 2002 (Ont. Sup. Ct.); *Canadian Blood*

Si l'ordonnance demandée avait été délivrée, il aurait fallu imposer certaines restrictions afin de protéger le droit à la vie privée des défendeurs non encore identifiés. L'empiètement sur la vie privée doit être circonscrit au maximum. L'ordonnance aurait précisé que seuls les pseudonymes pouvaient être utilisés dans la déclaration. Une annexe protégée par une ordonnance de confidentialité aurait été placée avec la déclaration, donnant les noms et adresses des clients des PSI qui correspondent aux pseudonymes. Finalement, l'ordonnance n'aurait pas exigé que les PSI souscrivent un affidavit à l'appui des renseignements trouvés.

LOIS ET RÈGLEMENTS

Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, ch. 5, art. 3, 4(3), 5, 7(3)(c),(d),(e),(h.2),(i), ann. 1.
Loi sur le droit d'auteur, L.R.C. (1985), ch. C-42, art. 27(2) (mod. par L.C. 1997, ch. 24, art. 15), 34(1) (mod., *idem*, art. 20), 37 (mod., *idem*), 80 (mod., *idem*, art. 50).
Règles de la Cour fédérale (1998), DORS/98-106, règles 41(1), 55, 81, 222, 232, 233, 238.

JURISPRUDENCE

DÉCISIONS APPLIQUÉES:

Norwich Pharmacal Co. v. Customs and Excise Comrs., [1974] A.C. 133 (H.L.); *Glaxo Wellcome PLC c. M.N.R.*, [1998] 4 C.F. 439; (1998), 162 D.L.R. (4th) 433; 7 Admin. L.R. (3d) 147; 20 C.P.C. (4th) 243; 81 C.P.R. (3d) 372; 228 N.R. 164 (C.A.); *Regina v. Maligne Building Ltd. et al.* (1980), 54 C.P.R. (2d) 11; 37 N.R. 526 (C.A.F.); *R. c. A. & A. Jewellers Limited*, [1978] 1 C.F. 479; [1977] C.T.C. 428 (1^{re} inst.); *Compo Company Ltd. c. Blue Crest Music Inc. et autres*, [1980] 1 R.C.S. 357; (1979), 105 D.L.R. (3d) 249; 45 C.P.R. (2d) 1; 29 N.R. 296; *CCH Canadian Ltée c. Barreau du Haut-Canada*, [2004] 1 R.C.S. 339; (2004), 226 D.L.R. (4th) 395; 30 C.P.R. (4th) 1; 317 N.R. 107; *R. c. Dymont*, [1988] 2 R.C.S. 417; (1988), 73 Nfld. & P.E.I.R. 13; 55 D.L.R. (4th) 503; 229 A.P.R. 13; 45 C.C.C. (3d) 244; 66 C.R. (3d) 348; 38 C.R.R. 301; 10 M.V.R. (2d) 1; 89 N.R. 249; *Irwin Toy Ltd. v. Doe* (2000), 12 C.P.C. (5th) 103 (C.S. Ont.).

DÉCISION EXAMINÉE:

MGM Studios, Inc. v. Grokster, Ltd., 259 F. Supp.2d 1029 (C.D. Cal. 2003).

DÉCISIONS CITÉES:

Ontario First Nations Limited Partnership v. John Doe, 3 juin 2002 (C.S. Ont.); *Canadian Blood Services/Société*

Services/Société Canadienne du Sang v. John Doe, June 17, 2002 (Ont. Sup. Ct.); *Wa'el Chehab v. John Doe*, October 3, 2003 (Ont. Sup. Ct.); *Kibale v. Canada*, [1991] F.C.J. No. 634 (T.D.) (QL); *Loblaw Companies Ltd. v. Aliant Telecom Inc.*, [2003] N.B.R. (2nd Supp.) No. 32 (Q.B.).

AUTHORS CITED

Copyright Board of Canada. *Copyright Board's Private Copying 2003-2004 Decision*, December 12, 2003.

World Intellectual Property Organization. *WIPO Performances and Phonograms Treaty*, Geneva, December 20, 1996.

MOTION for an order under rules 233 and 238 of the *Federal Court Rules, 1998* requiring certain internet service providers to disclose the identities of particular customers alleged to have infringed copyright by trading in recorded music downloaded from the internet. Motion denied.

APPEARANCES:

Ronald E. Dimock, Denis Sloan and Bruce Stratton for plaintiffs.

David A. van der Woerd for intervener, Electronic Frontier Canada.

Phillippa Lawson, Howard P. Knopf and Alex Cameron for intervener Canadian Internet Policy and Public Interest Clinic.

James A. Hodgson and Kathryn Podrebarac for non-party respondent Bell Canada.

Patrick Flaherty and Laura Malloni for non-party respondent Rogers Cable Communications Inc.

Charles F. Scott and Rocco Di Pucchio for non-party respondent Shaw Communications.

Joel D. Watson for non-party respondent Telus Communications.

Robert Bafaro for respondent.

SOLICITORS OF RECORD:

Dimock Stratton Clarizio LLP, Toronto, for plaintiffs.

Ross & McBride LLP, Hamilton, Ontario, for intervener Electronic Frontier Canada.

Canadian Internet Policy and Public Interest Clinic on its own behalf.

Canadienne du Sang v. John Doe, 17 juin 2002 (C.S. Ont.); *Wa'el Chehab v. John Doe*, 3 octobre 2003 (C.S. Ont.); *Kibale c. Canada*, [1991] A.C.F. n° 634 (1^{re} inst.) (QL); *Loblaw Companies Ltd. v. Aliant Telecom Inc.*, [2003] N.B.R. (2nd Supp.) n° 32 (B.R.).

DOCTRINE

Commission du droit d'auteur Canada. *Décision de la Commission du droit d'auteur pour la copie privée en 2003 et 2004*. 12 décembre, 2003.

Organisation mondiale de la propriété intellectuelle. *Traité de l'OMPI sur les interprétations et exécutions et les phonogrammes*. Genève, 20 décembre 1996.

REQUÊTE déposée en vertu des règles 233 et 238 des *Règles de la Cour fédérale (1998)* pour obtenir de certains prestataires de service Internet la divulgation de l'identité de certains clients qui auraient violé la législation sur les droits d'auteur en échangeant des œuvres musicales téléchargées d'Internet. Requête rejetée.

ONT COMPARU:

Ronald E. Dimock, Denis Sloan et Bruce Stratton pour les demandeurs.

David A. van der Woerd pour l'intervenant, Electronic Frontier Canada.

Phillippa Lawson, Howard P. Knopf et Alex Cameron pour l'intervenant, Clinique d'intérêt public et de politique d'Internet du Canada.

James A. Hodgson et Kathryn Podrebarac pour le défendeur non-partie, Bell Canada.

Patrick Flaherty et Laura Malloni pour le défendeur non-partie, Rogers Cable Communications Inc.

Charles F. Scott et Rocco Di Pucchio pour le défendeur non-partie, Shaw Communications.

Joel D. Watson pour le défendeur non-partie, Telus Communications.

Robert Bafaro pour le défendeur.

AVOCATS INSCRITS AU DOSSIER:

Dimock Stratton Clarizio LLP, Toronto, pour les demandeurs.

Ross & McBride LLP, Hamilton (Ontario), pour l'intervenant, Electronic Frontier Canada.

Clinique d'intérêt public et de politique d'Internet du Canada, pour son propre compte.

The following are the reasons for order and order rendered in English by

[1] VON FINCKENSTEIN J.: 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.C., 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 *MGM Studios, Inc. v. Grokster, Ltd.*, 259 F. Supp.2d 1029 (C.D. Cal. 2003), at pages 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,

Ce qui suit est la version française des motifs de l'ordonnance et ordonnance rendus par

[1] LE JUGE VON FINCKENSTEIN: Les demandeurs (ci-après CRIA) sont tous membres de l'industrie de l'enregistrement au Canada et ils présentent cette requête pour obtenir de cinq prestataires de service Internet, savoir Shaw Communications Inc., Rogers Cable Communications Inc., Bell Sympatico, Telus Inc. et Vidéotron Ltée (ci-après les PSI), la divulgation de l'identité de certains clients qu'ils soutiennent avoir violé la législation sur les droits d'auteur en échangeant illégalement des œuvres musicales téléchargées d'Internet.

[2] Les demandeurs ne peuvent déterminer les noms, adresses ou numéros de téléphone des 29 utilisateurs d'Internet en question, puisqu'ils ont adopté des pseudonymes associés au logiciel qu'ils utilisent, p. ex., Geekboy@KaZaA. Toutefois, ils ont mené une enquête qui, selon eux, leur a permis de découvrir que ces personnes ont utilisé des adresses du protocole d'Internet (adresses IP) qui sont assignées aux PSI défendeurs dans cette requête. Les demandeurs sollicitent une ordonnance en vertu des règles 233 et 238 des *Règles de la Cour fédérale (1998)*, DORS/98-106, pour obliger les PSI à divulguer les noms des clients qui ont utilisé les 29 adresses IP aux moments pertinents en l'espèce.

[3] Les demandeurs sont les plus grands producteurs d'œuvres musicales au Canada. Ils soutiennent que les 29 utilisateurs d'Internet ont chacun téléchargé sur leur ordinateur personnel plus de 1 000 chansons pour lesquelles les producteurs possèdent des droits d'auteur en vertu de la *Loi sur le droit d'auteur*, L.R.C. (1985), ch. C-42.

[4] Le processus de partage de fichiers entre homologues en vertu des logiciels Morpheus et Grokster est décrit de la façon suivante dans *MGM Studios, Inc. c. Grokster, Ltd.*, 259 F. Supp.2d 1029 (C.D. Cal. 2003), aux pages 1032 et 1033:

[TRADUCTION] Dans les deux cas, le logiciel peut être «téléchargé» sur l'ordinateur de l'utilisateur à partir des serveurs des défendeurs. Après l'installation, un utilisateur peut décider de «partager» certains fichiers enregistrés dans

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.

son ordinateur, notamment des fichiers d'œuvres musicales, des fichiers vidéo, des applications logicielles, des livres électroniques et des fichiers de textes. Dès que le logiciel est démarré sur l'ordinateur de l'utilisateur, il se relie automatiquement à un réseau d'homologues [. . .] ce qui permet de transférer les fichiers partagés disponibles à n'importe quel autre utilisateur relié au même réseau d'homologues.

Les logiciels Morpheus et Grokster offrent tous deux plusieurs moyens permettant à un utilisateur de faire une recherche dans le réservoir de fichiers partagés. Par exemple, un utilisateur peut limiter le champ aux fichiers audio et faire sa recherche en utilisant un mot clé, un titre ou un nom d'artiste. La recherche lancée, le logiciel affiche une liste (complète ou partielle) des usagers qui partagent des fichiers répondant aux critères donnés, ainsi qu'une estimation du temps requis pour le transfert de chaque fichier.

L'utilisateur demandeur peut alors cliquer sur une des options pour lancer le transfert de l'ordinateur source à son ordinateur personnel. Lorsque le transfert est terminé, le demandeur et la source ont des copies identiques du fichier. Le demandeur peut alors partager le fichier avec d'autres utilisateurs. L'ordinateur d'un utilisateur peut servir simultanément à des transferts multiples vers d'autres utilisateurs (téléchargements) ou à partir d'autres utilisateurs (téléchargements).

Les logiciels de partage de fichiers en cause ici, KaZaA et iMesh, fonctionnent essentiellement de cette façon.

[5] Les demandeurs soutiennent que cette façon de partager les fichiers constitue une violation de leurs droits à certaines œuvres musicales en vertu de la *Loi sur le droit d'auteur*. À l'exception de Vidéotron, les PSI soulèvent diverses objections à la demande d'ordonnance.

[6] Deux groupements d'intérêt public, la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) et La frontière électronique du Canada (EFC), ont reçu le droit d'intervenir pour présenter leurs points de vue.

[7] Les règles 232 et 238, ainsi que les articles pertinents de la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5 (LPRPDE), et de la *Loi sur le droit d'auteur*, sont reproduits à l'annexe 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 PIPEDA.
- The exceptions contained in PIPEDA apply in this case and an ISP by virtue of paragraph 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 Comrs.*, [1974] A.C. 133 (H.L.) and *Glaxo Wellcome PLC v. M.N.R.*, [1998] 4 F.C. 439 (C.A.) 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 instant case (albeit by naming John and Jane Doe as defendants), the plaintiff has to resort to rule 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

LES QUESTIONS EN LITIGE

[8] Cette requête soulève trois questions:

1. Quel est le critère juridique applicable?
2. Les demandeurs satisfont-ils à ce critère?
3. Si l'ordonnance est accordée, quels devraient être son libellé et sa portée?

Terrain d'entente

[9] Avant d'aborder ces questions, il y a lieu de faire remarquer que toutes les parties à cette requête sont d'accord sur les points suivants:

- Les clients des PSI ont une attente d'anonymat. Cette attente du respect de leur vie privée se fonde à la fois sur leurs contrats avec les PSI et sur les articles 3 et 5 de la LPRPDE.
- Les exceptions contenues dans la LPRPDE sont applicables en l'espèce et l'alinéa 7(3)c) de la LPRPDE porte que les PSI peuvent communiquer des renseignements personnels sans le consentement des intéressés, lorsque ces renseignements sont exigés par ordonnance d'un tribunal.

Question n° 1: Quel est le critère juridique applicable?

[10] Les arrêts *Norwich Pharmacal Co. v. Customs and Excise Comrs.*, [1974] A.C. 133 (H.L.), et *Glaxo Wellcome PLC c. M.R.N.*, [1998] 4 C.F. 439 (C.A.), ont établi que lorsqu'un demandeur potentiel recherche un interrogatoire préalable afin de connaître l'identité d'un défendeur, il peut avoir recours à l'interrogatoire préalable prévu en *equity*. Toutefois, lorsque l'action est déjà introduite (même si les défendeurs ne sont cités que sous les noms de John et Jane Doe), le demandeur doit s'en remettre à l'application des règles 233 et 238.

[11] La justification de cette procédure est exprimée succinctement par lord Reid dans l'arrêt *Norwich*, précité, à la page 175. Il déclare ceci:

[TRADUCTION] Tout bien considéré, je suis d'avis qu'ils appuient le point de vue des appelants. Je suis particulièrement

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 wrongdoing 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 Wellcome PLC, supra*, which followed *Norwich, supra*, and applied it in Canada, Stone J.A. described the preconditions for granting such relief at paragraphs 24-26 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

impressionné par les déclarations de lord Romilly M.R. et de lord Hatherley L.C. dans l'arrêt *Upmann c. Elkan* (1871) L.R. 12 Eq. 140; 7 Ch. App. 130. On y trouve le principe très raisonnable voulant que si, sans que ce soit sa faute, une personne est mêlée aux actes délictuels d'autres personnes et facilite ainsi le préjudice causé, elle n'engage peut-être pas sa responsabilité personnelle, mais elle est tenue d'aider la personne lésée en lui donnant tous les renseignements et en lui divulguant l'identité de l'auteur du préjudice. Je ne crois pas qu'il importe de savoir si son implication résulte d'un acte volontaire ou d'une obligation de faire ce qu'elle a fait. Il se peut que si elle a des frais, ils doivent être remboursés par la personne qui veut obtenir les renseignements. Mais la justice exige qu'elle coopère afin de réparer le préjudice causé si, sans le vouloir, elle l'a facilité.

[12] Dans l'arrêt *Glaxo Wellcome PLC*, précité, qui applique l'arrêt *Norwich*, précité, au Canada, le juge Stone, J.C.A., décrit ainsi les conditions préalables à l'octroi d'un tel redressement, aux paragraphes 24 à 26:

L'interrogatoire préalable prévu en *equity* est de nature discrétionnaire, mais dans l'arrêt *Norwich Pharmacal*, précité, la Chambre des lords a énuméré un certain nombre de considérations essentielles. À la page 199, lord Cross of Chelsea a dit que parmi les facteurs importants, il y avait:

[TRADUCTION] [. . .] la force de la preuve présentée par la demanderesse contre le présumé contrefacteur inconnu, la relation qui existe entre le présumé contrefacteur et l'intimé, la question de savoir si le renseignement peut être obtenu d'une autre source et la question de savoir si la communication du renseignement peut causer à l'intimé un préjudice qui ne pourrait pas être indemnisé au moyen du paiement des frais par la demanderesse.

Lord Kilbrandon a réitéré une bonne partie de ces considérations, à la page 205:

[TRADUCTION] Par conséquent, à mon avis, la Cour peut à bon droit ordonner aux intimés, par suite de la relation qu'ils entretiennent avec les appelantes, du fait des fonctions qui leur sont conférées par la loi et en raison des droits de propriété des appelantes, de communiquer aux appelantes les noms des personnes qui enfreignent les droits de ces dernières, selon ce que croient vraiment les appelantes, étant donné qu'ils constituent la seule source de renseignements possible permettant aux appelantes de savoir contre qui des poursuites peuvent être engagées, sous réserve de toute immunité que les intimés peuvent invoquer en leur qualité de ministère d'État.

Il me semble que la condition relative à l'existence d'une véritable demande que l'appelante peut présenter contre les

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

présomés auteurs du préjudice est destinée à assurer que les actions en vue d’un interrogatoire préalable ne soient pas intentées futillement ou sans justification. De même, le critère selon lequel les appelantes doivent entretenir une relation quelconque avec les intimés peut être interprété comme constituant une autre façon d’énoncer le principe selon lequel un simple témoin ou un tiers n’ayant rien à voir avec la présumée inconduite ne peut pas être assujéti à l’interrogatoire préalable. Je qualifierais donc ces considérations de conditions essentielles aux fins de l’interrogatoire préalable en *equity*.

Les passages susmentionnés des motifs de lord Cross of Chelsea et de lord Kilbrandon indiquent également que, selon une condition fondamentale, la personne devant faire l’objet de l’interrogatoire préalable doit être la seule source pratique de renseignements dont disposent les appelantes. Lord Reid a souligné l’importance de ce critère à la page 174, où il a tiré la conclusion suivante:

[TRADUCTION] Dans ce cas-ci, si les renseignements qui sont en la possession des intimés ne peuvent pas être communiqués maintenant au moyen d’un interrogatoire préalable, aucune action ne pourra être intentée parce que les appelantes ne savent pas qui sont les contrefacteurs. Les appelantes ne pourront donc jamais obtenir les renseignements.

En dernier lieu, la Chambre des lords a tenu compte de l’intérêt public tant en ce qui concerne la communication que la non-communication. À la page 175, lord Reid a maintenu que sa tâche consistait à [TRADUCTION] «établir l’équilibre entre le fait qu’il fallait rendre justice aux appelantes et les considérations avancées par les intimés à l’appui de la non-communication». À son avis, les commissaires étaient tenus de communiquer les noms des importateurs [TRADUCTION] «à moins qu’il n’existe une considération d’intérêt public les empêchant de le faire». La Chambre des lords a examiné la question sous divers angles. Les lords juristes ont reconnu qu’à cause de l’interdiction prévue par la loi en ce qui concerne la communication des noms des importateurs, l’intérêt public l’emporte peut-être sur le maintien du caractère confidentiel des renseignements. Ils ont reconnu que les importateurs peuvent donc s’attendre à ce que leurs noms demeurent confidentiels. L’intérêt public, en ce qui concerne la non-communication, a également été examiné du point de vue de l’État et compte tenu du fait que l’État a intérêt à assurer l’application et l’exécution efficaces de la législation en cause. En même temps, les lords juristes se rendaient compte que la communication des noms des importateurs peut fort bien servir l’intérêt public, lorsqu’il s’agit d’administrer la justice d’une façon équitable et efficace. Comme le vicomte Dilhorne l’a dit, à la page 188:

[TRADUCTION] Sous réserve de l’intérêt public voulant que le caractère confidentiel des renseignements fournis

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 *Glaxo 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 238(2) of the Rules 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

aux douanes soit protégé, à mon avis, l'intérêt public et le droit que possèdent les titulaires de brevets d'être protégés, lorsque la validité du brevet est reconnue et que la contrefaçon n'est pas contestée, exigent clairement que ces derniers soient en mesure d'obtenir d'une personne concernée qui n'a pas participé à la contrefaçon, au moyen d'un interrogatoire préalable, les noms et adresses des contrefacteurs.

[13] Selon moi, les arrêts *Norwich* et *Glaxo Wellcome* établissent que le critère qui permet d'ordonner un interrogatoire préalable en *equity* comprend les cinq volets suivants:

a) le demandeur doit démontrer qu'il existe à première vue quelque chose à reprocher à l'auteur inconnu du préjudice;

b) la personne devant faire l'objet d'un interrogatoire préalable doit avoir quelque chose à voir avec la question en litige—elle ne peut être un simple spectateur;

c) la personne devant faire l'objet de l'interrogatoire préalable doit être la seule source pratique de renseignements dont disposent les demandeurs;

d) la personne devant faire l'objet de l'interrogatoire préalable doit recevoir une compensation raisonnable pour les débours occasionnés par son respect de l'ordonnance portant interrogatoire préalable, en sus de ses frais de justice;

e) l'intérêt public à la divulgation doit l'emporter sur l'attente légitime de respect de la vie privée.

[14] Je ne vois pas pourquoi on n'appliquerait pas les mêmes principes lors d'une demande en vertu de la règle 238 dans le cas d'une action contre John Doe. L'exigence de signification prévue au paragraphe 238(2) des Règles pourrait alors faire l'objet d'une dispense d'observation en vertu de la règle 55, et elle le ferait sûrement.

[15] Les demandeurs fondent aussi leur requête sur la règle 233, mais cette disposition suppose l'existence de documents précis. Selon moi, la définition de 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 subsection 81(1) of the Rules, 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, pages 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 *Regina v. Maligne Building Ltd. et al.* (1980), 54 C.P.R. (2d) 11 (F.C.A.), at page 12:

que l'on trouve à la règle 222 n'a pas une portée suffisante pour englober la création de documents qu'une partie ne détient pas normalement et qu'on ne peut tirer des banques de données informatiques qu'utilise cette partie dans le cours ordinaire de ses affaires. En l'espèce, il n'existe pas de documents faisant le lien entre une adresse IP et un client donné d'un PSI. Bien sûr, si l'on obligeait un PSI à faire ce lien, de tels documents pourraient être créés. Ce n'est toutefois pas ce que prévoit la règle 233. En bref, la règle 233 a pour objectif d'ordonner la production de documents et non leur création.

Volet a: Le demandeur doit démontrer qu'il existe à première vue quelque chose à reprocher à l'auteur inconnu du préjudice

[16] Il y a trois lacunes dans la prétention des demandeurs qu'il existe à première vue quelque chose à reprocher à quelqu'un:

(i) Le contenu de l'affidavit est insuffisant

[17] Les affidavits de Gary Millin sur lequel les demandeurs s'appuient indiquent qu'aux époques en cause, il détenait le poste de président de MediaSentry Inc., une société qui offre une protection contre le piratage en ligne. Ses services ont été retenus par l'Association de l'industrie canadienne de l'enregistrement (CRIA) pour enquêter sur le partage de fichiers de chansons sur lesquelles les demandeurs ont un droit d'auteur. Dans son affidavit, M. Millin décrit le résultat des recherches de MediaSentry sur les activités de partage de fichiers par les 29 défendeurs non identifiés. M. Millin tient l'essentiel de ces renseignements de ses employés. Il s'agit donc en grande partie de ouï-dire. En vertu du paragraphe 81(1) des Règles, le ouï-dire et autres formes de renseignements fondés sur la conviction peuvent être admissibles, à condition que les motifs à l'appui soient énoncés. M. Millin ne dit pas sur quoi il fonde sa conviction, sauf à déclarer en contre-interrogatoire qu'en sa qualité que président de MediaSentry, [TRADUCTION] «une société employant de 20 à 25 personnes», il avait [TRADUCTION] «le contrôle général des affaires ainsi que des stratégies ciblées» (contre-interrogatoire Millin, pages 6 et 8, lignes 16 et 18 respectivement). C'est insuffisant. Comme le dit le

juge Heald dans l'arrêt *Regina c. Maligne Building Ltd. et al.* (1980), 54 C.P.R. (2d) 11 (C.A.F.), à la page 12:

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

Lorsqu'un affidavit mis en preuve repose sur des renseignements et sur une conviction, il importe de préciser la source des renseignements.

[18] Moreover, subsection 81(2) of the Rules provides:

[18] De plus, le paragraphe 81(2) des Règles porte que:

81. . . .

81. [. . .]

(2) 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 material facts.

(2) Lorsqu'un affidavit contient des déclarations fondées sur ce que croit le déclarant, le fait de ne pas offrir le témoignage de personnes ayant une connaissance personnelle des faits substantiels peut donner lieu à des conclusions défavorables.

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 *R. v. A. & A. Jewellers Limited*, [1978] 1 F.C. 479 (T.D.), at page 480:

Il semble clair que d'autres employés de MediaSentry étaient mieux placés pour souscrire les affidavits en cause et pour répondre aux questions des défendeurs en contre-interrogatoire. M. Millin aurait dû, au strict minimum, identifier les employés ayant fait le travail, énoncer leurs compétences et expliquer sous quelle forme ils lui avaient transmis les résultats de leurs enquêtes. Parlant de la règle 81, le juge en chef adjoint Thurlow déclare ceci dans l'arrêt *R. c. A. & A. Jewellers Limited*, [1978] 1 C.F. 479 (1^{re} inst.), à la 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.]

La Cour a droit à la déclaration sous serment d'une personne qui a une connaissance personnelle des faits, lorsque ladite personne peut la fournir. La deuxième partie de la Règle est purement facultative, et doit être utilisée seulement lorsque la meilleure des preuves, à savoir la déposition sous serment de la personne qui sait, ne peut pas être obtenue immédiatement, pour des raisons admissibles ou évidentes. [Non souligné dans l'original.]

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.

On ne trouve aucune raison de cette nature dans les affidavits de M. Millin ou dans son contre-interrogatoire qui justifierait une entorse à la règle de la meilleure preuve.

[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

[19] M. Millin a aussi témoigné que sa société fournit le service dit MediaDecoy, qui distribue des fichiers fantômes inopérants par l'entremise d'Internet. Les personnes qui les téléchargeaient croient, à tort, qu'il s'agit de fichiers d'œuvres musicales. Les fichiers sont conçus pour ressembler à des œuvres musicales, mais ils

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 (affidavit of Mr. Millin in motion materials related to Shaw, at paragraph 24):

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.

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

sont inopérants. À la question de savoir s’il savait si certains des fichiers présumément copiés par les violateurs présumés provenaient de MediaDecoy, M. Millin a répondu qu’il n’avait écouté aucun des fichiers copiés par les violateurs présumés et que l’écoute des fichiers n’était pas prévue dans son contrat ou dans [TRADUCTION] «le processus mis en place avec CRIA» (contre-interrogatoire Millin, QQ 107-107, 189-196). Cette preuve à distance est bien loin de satisfaire aux prescriptions de la règle 81. Par conséquent, la Cour n’a été saisie d’aucune preuve que les fichiers rendus disponibles pour le téléchargement sont des contrefaçons des fichiers des demandeurs.

(ii) Il n’y a aucune preuve établissant un lien entre les pseudonymes et les adresses IP

[20] Comme je l’ai déjà mentionné, les demandeurs veulent que les PSI leur communiquent les noms de leurs clients qui ont utilisé certaines adresses IP à des moments précis. Toutefois, les affidavits de M. Millin et son contre-interrogatoire n’apportent aucune preuve claire et détaillée de comment on a établi un lien entre les pseudonymes des utilisateurs de KaZaA ou iMesh et les adresses IP identifiées par MediaSentry. Par exemple, voici ce que déclare M. Millin dans son affidavit au sujet d’un des 29 pseudonymes (affidavit de M. Millin, documents sur Shaw déposés avec la requête, paragraphe 24):

[TRADUCTION] MediaSentry a aussi conclu que l’adresse IP de Geekboy@KaZaA au moment où elle faisait son enquête était 24.84.179.98. L’American Registry for Internet Numbers (ARIN), l’organisation à but non lucratif qui assigne les adresses IP aux prestataires de service Internet (PSI) donne un accès public à sa banque de données sur les adresses IP (www.arin.net). Cette banque de données indique que ARIN avait assigné l’adresse IP 24.84.179.98 à Shaw Communications Inc. [. . .]

Aucune preuve n’indique comment le pseudonyme «Geekboy@KaZaA» a été lié à l’adresse IP 24.84.179.98. En l’absence de toute preuve démontrant comment l’adresse IP 24.84.179.98 a mené à Geekboy@KaZaA, et sans la conviction qu’une telle preuve est fiable, la Cour agirait de façon irresponsable en ordonnant la divulgation du nom du client correspondant

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, at para. 10);
- b. copied files to “shared directories” on their computers (Millin, at para. 9);
- c. used ISP services to connect their computers to the Internet (Millin, at para.16);
- d. ran the peer-to-peer application on their computers while in the Internet (Millin, at 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, at 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

à l'adresse IP 24.84.179.98, l'exposant ainsi à une poursuite initiée par les demandeurs.

(iii) Il n'y a aucune preuve de violation du droit d'auteur

[21] Les demandeurs affirment, au paragraphe 84 de leurs prétentions écrites, que leur preuve démontre que les violateurs présumés ont:

[TRADUCTION]

- a. installé un logiciel de partage des fichiers entre homologues sur leurs ordinateurs (Millin, paragraphe 10);
- b. copié des fichiers sur des «répertoires partagés» sur leurs ordinateurs (Millin, paragraphe 9);
- c. utilisé les services des PSI pour relier leurs ordinateurs à Internet (Millin, paragraphe 16);
- d. fait fonctionner le logiciel de partage des fichiers entre homologues sur leurs ordinateurs alors qu'ils étaient connectés à Internet (Millin, paragraphe 16); et
- e. rendu les fichiers des répertoires partagés disponibles pour leur copie, transmission et distribution à n'importe lequel des millions d'utilisateurs du service de partage des fichiers entre homologues (Millin, paragraphe 22).

[22] Au paragraphe 102 de leurs prétentions écrites, ils soutiennent que ces activités constituent une violation de la *Loi sur le droit d'auteur* pour les motifs suivants:

[TRADUCTION]

- a. **la reproduction** d'enregistrements sonores par les violateurs présumés (paragraphe 18(1) et 27(1));
- b. **l'autorisation** de reproduire des enregistrements sonores (paragraphe 18(1) et 27(1));
- c. **la mise en circulation** de copies non autorisées des enregistrements sonores de façon à porter préjudice aux demandeurs (alinéa 27(2)b)); et
- d. **la possession** de copies non autorisées que les violateurs présumés savaient, ou devaient savoir, être des contrefaçons, dans le but de les mettre en circulation, comme il est mentionné plus tôt (alinéa 27(2)d)).

[23] Ces prétentions doivent être confrontées à la nature de la législation régissant le droit d'auteur. Le droit d'auteur ne peut être invoqué que dans les cas énoncés explicitement dans le texte législatif. Une cour

are not provided for in the statute. As Estey J. stated in *Compo Company Ltd. v. Blue Crest Music Inc. et al.*, [1980] 1 S.C.R. 357, at pages 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] Subsection 80(1) [as am. by S.C. 1997, c. 24, s. 50] 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,

. . .

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.

[25] Thus, downloading a song for personal use does not amount to infringement. See *Copyright Board's, 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 users via a P2P service.

ne peut déduire ou créer des droits non mentionnés dans le texte législatif. Comme le dit le juge Estey, dans l'arrêt *Compo Company Ltd. c. Blue Crest Music Inc. et autres*, [1980] 1 R.C.S. 357, aux pages 372 et 373:

[. . .] le droit d'auteur n'est pas régi par les principes de la responsabilité délictuelle ni par le droit de propriété mais par un texte législatif. Il ne va pas à l'encontre des droits existants en matière de propriété et de conduite et il ne relève pas des droits et obligations existant autrefois en *common law*. La loi concernant le droit d'auteur crée simplement des droits et obligations selon certaines conditions et circonstances établies dans le texte législatif. En droit anglais, il en est ainsi depuis la reine Anne, sous laquelle fut promulguée la première loi relative au droit d'auteur. Il n'est pas utile, aux fins de l'interprétation législative, d'introduire les principes de la responsabilité délictuelle. La loi parle d'elle-même et c'est en fonction de ses dispositions que doivent être analysés les actes de l'appelante.

La Cour doit donc analyser les prétentions écrites des demandeurs au vu de l'arrêt *Compo Co.*, précité.

[24] Le paragraphe 80(1) [mod. par L.C. 1997, ch. 24, art. 50] de la *Loi sur le droit d'auteur* est rédigé comme suit:

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

[25] Par conséquent, le fait de télécharger une chanson pour usage privé ne constitue pas une violation du droit d'auteur. Voir *Décision de la Commission du droit d'auteur pour la copie privée en 2003-2004*, 12 décembre 2003, à la page 20.

[26] On n'a déposé aucune preuve que les violateurs présumés auraient distribué des enregistrements sonores ou autorisé leur reproduction. Ils ont simplement placé leurs propres copies dans les répertoires partagés accessibles à d'autres utilisateurs par l'entremise d'un service de partage de fichiers entre homologues.

[27] As far as authorization is concerned, the case of *CCH Canadian Ltd. v. Law Society of Upper Canada*, [2004] 1 S.C.R. 339 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* [at page 361]:

“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

[27] S’agissant de l’autorisation, l’arrêt *CCH Canadienne Ltée c. Barreau du Haut-Canada*, [2004] 1 R.C.S. 339, a précisé que le fait de mettre sur place des appareils qui permettent de faire des copies ne correspond pas à autoriser la violation du droit d’auteur. Je ne peux voir quelle réelle différence pourrait exister entre une bibliothèque qui place une photocopieuse dans une pièce remplie de documents visés par le droit d’auteur et un utilisateur qui place sa propre copie dans un répertoire partagé relié à un service de partage de fichiers entre homologues. Dans les deux cas, les conditions nécessaires à la copie et à la contrefaçon sont présentes, mais il manque l’autorisation. Voici ce que déclare la juge en chef McLachlin à ce sujet dans l’arrêt *CCH*, précité [à la page 361]:

«Autoriser» signifie «sanctionner, appuyer ou soutenir» («*sanction, approve and countenance*»): *Muzak Corp. c. Composers, Authors and Publishers Association of Canada Ltd.*, [1953] 2 R.C.S. 182, p. 193; *De Tervagne c. Beloeil (Ville)*, [1993] 3 C.F. 227 (1^{re} inst.). Lorsqu’il s’agit de déterminer si une violation du droit d’auteur a été autorisée, il faut attribuer au terme «*countenance*» son sens le plus fort mentionné dans le dictionnaire, soit [TRADUCTION] «*approuver, sanctionner, permettre, favoriser, encourager*»: voir *The New Shorter Oxford English Dictionary* (1993), vol. 1, p. 526. L’autorisation est néanmoins une question de fait qui dépend de la situation propre à chaque espèce et peut s’inférer d’agissements qui ne sont pas des actes directs et positifs, et notamment d’un degré suffisamment élevé d’indifférence: *CBS Inc. c. Ames Records & Tapes Ltd.*, [1981] 2 All E.R. 812 (Ch. D.), p. 823-824. Toutefois, ce n’est pas autoriser la violation du droit d’auteur que de permettre la simple utilisation d’un appareil susceptible d’être utilisé à cette fin. Les tribunaux doivent présumer que celui qui autorise une activité ne l’autorise que dans les limites de la légalité: *Muzak*, précité. Cette présomption peut être réfutée par la preuve qu’il existait une certaine relation ou un certain degré de contrôle entre l’auteur allégué de l’autorisation et les personnes qui ont violé le droit d’auteur: *Muzak*, précité; *De Tervagne*, précité. Voir également J. S. McKeown, *Fox Canadian Law of Copyright and Industrial Designs* (4^e éd. (feuilles mobiles)), p. 21-104 et P. D. Hitchcock, «Home Copying and Authorization» (1983), 67 C.P.R. (2d) 17, p. 29-33.

[28] Le simple fait de placer une copie dans un répertoire partagé où l’on peut y avoir accès par l’entremise d’un service de partage de fichiers entre homologues n’est pas de la distribution. La distribution implique un acte positif de la part du propriétaire du

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. *WIPO Performances and Phonograms Treaty*, Geneva, December 20, 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 subsection 27(2) [as am. by S.C. 1997, c. 24, s. 15] 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 definitely 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

répertoire partagé, comme l'envoi de copies ou le fait d'annoncer qu'elles sont disponibles pour qui veut les copier. En l'espèce, aucune telle preuve n'a été présentée par les demandeurs. Ils ont simplement présenté en preuve le fait que les violateurs présumés ont mis des copies à disposition sur leurs répertoires partagés. Le droit exclusif de mettre à disposition est prévu dans Organisation mondiale de la propriété intellectuelle. *Traité de l'OMPI sur les interprétations et exécutions et les phonogrammes*, Genève, 20 décembre 1996. Ce traité n'a toutefois pas encore été ratifié par le Canada et il ne fait donc pas partie de la législation canadienne sur le droit d'auteur.

[29] Finalement, les demandeurs soutiennent qu'il y a eu violation à une étape ultérieure, contrairement au paragraphe 27(2) [mod. par L.C. 1997, ch. 24, art. 15] de la *Loi sur le droit d'auteur*, mais ils n'ont présenté aucune preuve que le violateur en avait connaissance. La preuve de cette connaissance est une condition essentielle pour démontrer qu'il y a contrefaçon en vertu de cet article.

Volet b: La personne devant faire l'objet d'un interrogatoire préalable doit avoir quelque chose à voir avec la question en litige—elle ne peut être un simple spectateur

[30] En l'espèce, les demandeurs satisfont à l'exigence énoncée à d) du paragraphe 22 ci-haut. En tant que fournisseurs d'accès Internet, les PSI ont très certainement un lien avec les violateurs présumés. Ils ne sont pas de simples spectateurs. C'est par leur entremise que les personnes qui font du téléchargement et du téléchargement accèdent à Internet et entrent en contact.

Volet c: La personne devant faire l'objet de l'interrogatoire préalable doit être la seule source pratique de renseignements dont disposent les demandeurs

[31] En l'espèce, les présumés auteurs du préjudice utilisent les logiciels KaZaA, KaZaA Lite ou iMesh, qu'ils ont téléchargés des sites web du même nom. Les affidavits de Gary Millin et de Kathy Yonekura ne spécifient aucunement qui gère ces sites web et où ils sont situés, non plus qu'ils abordent la question de savoir si les personnes qui gèrent ces sites web pourraient leur

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.

fournir les noms qui correspondent aux pseudonymes. En l'absence d'une telle preuve, la Cour ne peut déterminer si les PSI sont la seule source pratique de renseignements dont disposent les demandeurs.

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

Volet d: La personne devant faire l'objet de l'interrogatoire préalable doit recevoir une compensation raisonnable pour les débours occasionnés par son respect de l'ordonnance portant interrogatoire préalable, en sus de ses frais de justice

[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.

[32] Les affidavits déposés par Telus, Shaw, Rogers, Bell et EFC démontrent qu'il n'est pas facile de trouver le nom et l'adresse du client qui a utilisé une adresse IP à un moment précis.

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

[33] À titre d'exemple, voici comment David Shrimpton de Telus décrit le processus:

[TRADUCTION]

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.

16. Pour essayer d'obtenir les renseignements demandés, les employés de TELUS devront faire une recherche dans au moins trois banques de données et faire concorder ce qu'ils ont trouvé pour localiser le client probable. Ce processus ne faisant pas partie de notre cadre normal d'opération, il n'y a pas de listes, dossiers ou documents qui contiennent ces renseignements. De plus, aucune personne à l'emploi de TELUS ne possède ces renseignements dans le cadre de ses fonctions. TELUS ne s'intéresse pas à ce que ses clients font sur 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.

17. La seule façon de savoir quel client s'est connecté à Internet via l'adresse IP en cause serait de faire concorder l'adresse IP aux dates, heures, réseaux et fuseaux horaires appropriés à une banque de données des codes d'authentification des messages (adresse MAC) et, ensuite, de faire concorder ce résultat avec la banque de données de la clientèle. Ceci suppose que ces renseignements existent toujours et qu'ils peuvent être récupérés. Comme je l'indique ci-après, plus une recherche porte sur un point éloigné dans le temps, moins les renseignements seront fiables étant donné qu'ils sont conservés de façon différente selon les systèmes utilisés.

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.

18. TELUS est prestataire de service Internet essentiellement en Alberta et en Colombie-Britannique, mais nous avons aussi des clients dans les autres provinces et territoires. Le service Internet de TELUS a 750 000 clients privés et il dessert 85 000 institutions, organisations gouvernementales et sociétés. Ce chiffre ne comprend que les clients privés et les petites entreprises.

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

19. L’American Registry for Internet Numbers (ARIN) assigne un certain nombre d’adresses IP à TELUS. Il y a toutefois moins d’adresses IP que de clients. Tous les PSI sont dans cette situation. Le système d’adresses IP se fonde sur l’hypothèse que tous les utilisateurs potentiels d’Internet ne se connecteront pas au même moment. En conséquence, la plupart des adresses IP ont un caractère dynamique, ce qui veut dire qu’elles ne sont pas associées à un ordinateur personnel (PC) précis. En fait, lorsqu’un client se connecte à Internet, le matériel informatique auquel le PC en cause est relié «demande» une adresse IP et le système lui en «assigne» une pour l’occasion. Il s’ensuit que le lien entre une adresse IP et un client donné peut être très bref. En quelques heures, une adresse IP peut être assignée à plusieurs utilisateurs de façon consécutive. Étant donné que la fréquence et la durée des visites varient d’un utilisateur à l’autre, les adresses IP ne sont pas assignées aux adresses MAC de façon séquentielle. Cette fonctionnalité fait que les adresses IP ne sont associées à aucun client précis ou assignées selon une configuration prédéterminée. (Le mot «adresse IP» peut causer une certaine confusion selon le sens ordinaire, puisqu’il ne s’agit pas vraiment d’une adresse comme peut en avoir une maison.) Il n’est donc pas possible d’identifier un client à partir de la seule adresse IP. De plus, il n’est pas facile de retrouver une adresse IP.

20. Le fait que ce n’est pas le PC lui-même qui a une adresse, mais plutôt le matériel de connexion, savoir le routeur ou la carte réseau, qui permet au PC de se connecter à Internet qui a reçu une adresse permanente lors de sa première connexion à Internet, ne facilite pas non plus les choses. C’est ce qu’on appelle l’adresse MAC et elle est associée au matériel de connexion et non au PC. Cette distinction a son importance, surtout lorsque le matériel de connexion sert à plusieurs PC reliés à un réseau local (LAN), comme je l’explique ci-après.

21. Donc, pour identifier le client, TELUS doit d’abord trouver l’adresse MAC à laquelle on a assigné l’adresse IP en cause à un moment précis dans le temps.

22. Notons que TELUS ne peut jamais connaître «l’utilisateur», savoir la personne qui est à l’ordinateur au moment de la prétendue violation. TELUS peut seulement dire qui a ouvert le compte TELUS associé à une adresse MAC. Comme je l’expliquerai plus loin, le titulaire du compte et l’utilisateur ne sont pas nécessairement une seule et même personne. Ils peuvent même ne pas se connaître du tout. S’agissant du titulaire du compte, si la demande de renseignements est présentée dans les 30 jours de la connexion à Internet pour partager des fichiers, TELUS à une bonne chance de le retrouver (selon toutefois le système Internet TELUS utilisé). Toutefois, pour une demande portant sur une

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 La Forest J. in *R. v. Dymnt*, [1988] 2 S.C.R. 417, at page 427:

activité réalisée depuis plus de 30 jours, les renseignements deviennent si peu fiables qu'on peut dire qu'ils n'existent pas vraiment.

[34] Sans entrer dans les détails techniques fournis par chaque PSI, on peut tirer les conclusions générales suivantes de la preuve présentée par les PSI au sujet des renseignements en cause:

- ces renseignements ne sont généralement pas recueillis par les PSI, et il faut une opération spécifique pour les extraire de leurs banques de données;

- plus les renseignements datent, plus il est difficile de les extraire. Les données peuvent être sauvegardées sur bande ou même supprimées, selon leur date d'entrée;

- plus les renseignements datent, plus les résultats obtenus des tentatives d'extraction des données perdent en fiabilité;

- avec le temps, il peut devenir impossible de faire le lien entre certaines adresses IP et les clients;

- au mieux, les PSI peuvent retrouver les clients en cause, mais ils ne pourraient jamais connaître le nom du vrai utilisateur. Par exemple, une adresse IP peut permettre d'identifier un client, mais il peut s'agir d'une institution ou d'un réseau local accessible à plusieurs utilisateurs.

[35] Il est clair que le processus qu'on veut imposer aux PSI serait coûteux et qu'il les obligerait à prélever des ressources affectées à d'autres tâches. Comme les PSI ne sont aucunement responsables des violations présumées, il faudrait leur rembourser les coûts raisonnables liés à la divulgation de l'identité de leurs clients, en sus de frais associés à la présente requête.

Volet e: L'intérêt public à la divulgation doit l'emporter sur l'attente légitime de respect de la vie privée

[36] Il va sans dire que la protection de la vie privée a une importance majeure pour la société canadienne. Comme le dit le juge La Forest dans l'arrêt *R. c. Dymnt*, [1988] 2 R.C.S. 417, à la page 427:

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 Ltd. v. Doe* (2000), 12 C.P.C. (5th) 103 (Ont. Sup. Ct.) stated, at paragraphs 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. Paragraph 7(3)(c) allows disclosure without consent if such disclosure is:

Fondée sur l'autonomie morale et physique de la personne, la notion de vie privée est essentielle à son bien-être. Ne serait-ce que pour cette raison, elle mériterait une protection constitutionnelle, mais elle revêt aussi une importance capitale sur le plan de l'ordre public.

[37] S'agissant plus particulièrement d'Internet, dans *Irwin Toy Ltd. c. Doe* (2000), 12 C.P.C. (5th) 103 (C.S. Ont.), le juge Wilkins déclare ceci aux paragraphes 10 et 11:

[TRADUCTION] La circulation des renseignements via Internet sous le couvert d'un nom d'emprunt ou d'un pseudonyme s'appuie implicitement sur une compréhension partagée du fait que l'identité de la source restera jusqu'à un certain point confidentielle. Certains prestataires de service Internet informent leurs clients qu'ils respecteront leur droit à la vie privée. Certains vont même jusqu'à faire procéder à l'examen de leur politique de protection de la vie privée et à en faire vérifier l'application. En général, il est entendu qu'on ne divulgue pas l'adresse IP d'un client. Il semble que certains prestataires de service Internet exigent que leurs clients s'engagent à ne pas envoyer de messages diffamatoires, et qu'ils prennent en contrepartie des mesures raisonnables pour préserver l'anonymat de la source de renseignements.

Conformément au protocole ou à l'étiquette Internet, il y a une sécurité importante rattachée à une certaine garantie de confidentialité lorsqu'il s'agit de l'adresse IP de la source d'un message. Cette réalité respecte aussi ce que l'on peut concevoir comme une bonne politique d'intérêt public. En autant que je sache, le prestataire de service Internet n'a aucune obligation de fournir, volontairement ou sur demande, le nom de la personne associée à une adresse IP.

[38] Le législateur a aussi reconnu qu'il fallait protéger la vie privée en adoptant la LPRPDE, dont l'un des objectifs majeurs est d'assurer le droit de chacun de contrôler la collecte, l'utilisation et la communication de renseignements personnels dans le secteur privé (article 3).

[39] Toutefois, bien que la législation protège le droit de chacun à la vie privée, ce droit ne peut être invoqué par une personne pour échapper à sa responsabilité, civile ou criminelle. En conséquence, rien dans la LPRPDE ne vient limiter la compétence de la Cour d'ordonner la production de documents relatifs à l'identité des personnes. L'alinéa 7(3)c) autorise la communication sans le consentement de l'intéressé lorsque:

7. (3) . . .

(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*, *supra* and *Glaxo*, *supra*, 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*, *supra*; *Ontario First Nations Limited Partnership v. John Doe* (3 June 2002) (Ont. Sup. Ct.); *Canadian Blood Services/Société Canadienne du Sang v. John Doe* (June 17, 2002) (Ont. Sup. Ct.); *Wa'el Chehab v. John Doe* (October 3, 2003) (Ont. Sup. Ct.); *Kibale v. Canada*, [1991] F.C.J. No. 634 (T.D.) (QL); *Loblaw Companies Ltd. v. Aliant Telecom Inc.*, [2003] N.B.R. (2d Supp.) No. 32 (Q.B.).

[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, 2004. This clearly makes the information more difficult to obtain, if it can be obtained

7. (3) [. . .]

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. [Non souligné dans l'original.]

[40] Donc, tant la LPRPDE que le critère de *Norwich*, précité; et *Glaxo*, précité exigent que la Cour recherche un équilibre entre le droit à la vie privée, les droits des tiers et l'intérêt public.

[41] Cette requête n'est pas novatrice. Par le passé, des tiers se sont vu imposer l'obligation de communiquer des documents contenant les nom et adresse d'un défendeur dont on ne connaissait que l'adresse du protocole d'Internet. Il n'y a pas de jurisprudence où les préoccupations relatives à la vie privée et autres préoccupations face à une divulgation auraient pris le pas sur l'intérêt à l'obtention des documents et renseignements nécessaires à l'identification des défendeurs. Voir: *Irwin Toy v. Doe*, précité; *Ontario First Nations Limited Partnership v. John Doe* (3 juin 2002) (C.S. Ont.); *Canadian Blood Services/Société canadienne du Sang v. John Doe* (17 juin 2002) (C.S. Ont.); *Wa'el Chehab v. John Doe* (3 octobre 2003) (C.S. Ont.); *Kibale c. Canada*, [1991] A.C.F. n° 634 (1^{re} inst.) (QL); *Loblaw Companies Ltd. c. Aliant Telecom Inc.* [2003] N.B.R. (2d Supp.) n° 32 (B.R.).

[42] En l'espèce, les demandeurs ont un droit d'auteur légitime sur leurs œuvres et ils ont le droit d'être protégés de toute violation. Toutefois, avant de rendre l'ordonnance appropriée, la Cour doit être convaincue de façon évidente que les renseignements qui seraient divulgués sont fiables, et elle doit limiter la divulgation à ce qui est absolument nécessaire pour que les demandeurs puissent identifier les défendeurs présumés. Toute ordonnance de cette nature devrait aussi, au vu des droits des défendeurs à la protection de leur vie privée, être assortie des restrictions et mesures de confidentialité que la Cour juge appropriées. Tous les PSI ont convenu qu'ils peuvent produire les renseignements demandés en temps utile. En l'espèce, la preuve a été collectée en octobre, novembre et décembre 2003. L'avis de requête demandant la divulgation par les PSI n'a été déposé que le 11 février 2004. Il est donc clair que les

at all, and decreases its reliability. No explanation was given by the plaintiffs as to why they did not move earlier than February 2004. 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.

renseignements en cause sont plus difficiles à obtenir, si même on peut le faire, et que leur fiabilité est réduite. Les demandeurs n'ont pas expliqué pourquoi ils n'ont pas procédé avant février 2004. Dans de telles circonstances, au vu de l'ancienneté des données, de leur peu de fiabilité et de la possibilité qu'on communique l'identité d'un client innocent, la Cour est d'avis que le respect de la vie privée prime l'intérêt public à la divulgation.

Question n° 2: Les demandeurs satisfont-ils à ce critère?

[43] Au vu de ce qui précède, il est clair selon moi que les demandeurs n'ont pas:

- établi qu'il existe à première vue un fondement à leurs prétentions (le contenu de leur affidavit est insuffisant; ils n'ont pas établi un lien de causalité entre les pseudonymes utilisés lors du partage de fichiers entre homologues et les adresses IP; et ils n'ont pas établi à première vue qu'il y aurait contrefaçon);

- démontré que les PSI sont la seule source pratique pour obtenir l'identité des utilisateurs de pseudonymes utilisés lors du partage de fichiers entre homologues; et

- démontré que l'intérêt public à la divulgation prime le respect de la vie privée, compte tenu de l'ancienneté des données.

Ils n'ont donc pas satisfait au critère énoncé au paragraphe 13 des présents motifs.

Question n° 3: Si l'ordonnance est accordée, quels devraient être son libellé et sa portée?

[44] Si j'avais délivré l'ordonnance demandée, il m'aurait fallu imposer certaines restrictions afin de protéger le droit à la vie privée des défendeurs non encore identifiés. Premièrement, les identités révélées n'auraient pu être utilisées que dans le cadre du présent litige. Je ne vois pas pourquoi les demandeurs auraient été exemptés de la règle de l'engagement implicite, comme ils l'ont demandé. L'empiètement sur la vie privée doit être circonscrit au maximum. Comme les demandeurs recherchaient quels noms ils pouvaient substituer à ceux de John et Jane Doe, on ne pouvait en autoriser la divulgation qu'à cette fin.

[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.

[45] Deuxièmement, afin de limiter encore plus l'empiètement sur la vie privée des clients des PSI, l'ordonnance aurait précisé que seuls les pseudonymes pouvaient être utilisés dans la déclaration. Une annexe protégée par une ordonnance de confidentialité aurait été placée avec la déclaration, donnant les noms et adresses des clients des PSI qui correspondent aux pseudonymes.

[46] Finalement, l'ordonnance n'aurait pas exigé que les PSI souscrivent un affidavit à l'appui des renseignements trouvés. Pour que les demandeurs puissent procéder, il aurait suffi qu'on divulgue le nom, et la dernière adresse connue, des défendeurs.

[47] Au vu de ma conclusion sur la question n° 2, cette requête ne peut être accueillie.

ORDONNANCE

1. La requête est rejetée.
2. Tous les PSI défendeurs ont droit aux dépens.
3. Les intervenants n'ont pas droit aux dépens.

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.

...

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.

...

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.

...

(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.

Personal Information Protection and Electronic Documents Act, S.C. 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

Annexe A

Règles de la Cour fédérale (1998), DORS/98-106

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) 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) 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) 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.

Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, ch. 5.

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

disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

...

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.

...

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.

...

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

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) Toute disposition de la présente partie s'applique malgré toute disposition—éditée 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) 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) 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

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.

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

...

4.3.1

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 ...

...

4.3.5

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

...

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. ...

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.

LPRPDE: Annexe 1—Principes énoncés dans la Norme nationale du Canada intitulée Code type sur la protection des renseignements personnels, CAN/CSA-Q830-96

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

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

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

[...]

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. [...]

27. . . .

(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),

. . .

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.

. . .

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.

. . .

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.

(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;

27. [. . .]

(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) 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. 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. 37.

[. . .]

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

(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'œuvre musicale ou de la prestation d'une œuvre musicale qui le constituent, sur un support audio pour les usages suivants:

a) vente ou location, ou exposition commerciale;

- (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.

- b) distribution dans un but commercial ou non;
- c) communication au public par télécommunication;
- d) exécution ou représentation en public.