Canadian Filesharing Lawsuit: Motion to Disclose

[**Disclaimer:** This is my blog of CRIA's motion to disclose the identities of twenty-nine of the subscribers of five national ISPs in Canada. I attended and was present at the hearing in Toronto and the subsequent tele-hearing in Ottawa as a member of the CIPPIC legal team, in the capacity of a law student, and am therefore not a disinterested party. This is NOT a transcript of what was said and by whom nor do I pretend to be objective. My personal interest (and background) is biased towards CIPPIC's position in this case and I freely admit such. Nonetheless, I have tried to be as accurate and complete as possible. Comments and questions about this blog should be directed to Jason Young at copyright2@lexinformatica.org.]

Day 1, March 12, 2004, Toronto

Plaintiff
Canadian Recording Industry Association (representing the music labels)

Non-party respondents
Shaw, Telus, Rogers, Bell, Videotron (also served, but chose not to oppose the motion and was not present)

Interveners
Canadian Internet Policy and Public Interest Clinic (CIPPIC), Eectronic Frontiers Canada (EFC)

Motion to Strike Affidavit of Gary Millin, President, MediaSentry

Scott, Charles: Counsel for Shaw first tried to strike the affidavit of MediaSentry president Gary Millin under r. 80(1) for lack of personal knowledge as to the evidence. If this affidavit is struck, there is no evidence and the motion will fail.

von Finckenstein J: Why shouldn't I just treat this adversely instead of striking?

Stratton, Bruce (counsel for the plaintiff CRIA): (Responded).

Scott, C.: asked the judge through Millin's affidavit and showed him where Millin admitted that he had no personal knowledge as to the evidence he provided.

von Finckenstein J: Neither of you have cited any law; I'm going to take this under reserve.

Main Motion

Dimock, Ronald (counsel for the plaintiff CRIA)**:** If we don't succeed we will be non-suited. Our clients are facing significant problems. We are not trying the infringement today, that is for another day. The ISPs hold the key to identifying the defendants.

The first issue is the test. The duty is on the ISPs to disclose this information. Where there is no evidence of an overriding (public interest) principle, the duty prevails. We

only need to show a *prima facie* or *bona fide* case. It is sufficient for the purposes of this motion at this stage to merely show an arguable case.

On the matter of privacy, the issue has been raised by the interveners and some of the ISPs. The users had clear expectations that their privacy is not sacrosanct. There is a clear expectation that their information can be disclosed in certain circumstances. There is no circumscription of these activities by the *Charter of Rights and Freedoms* (the "*Charter*") or by *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). The data (we are seeking) is in some cases somewhat dated, but other organizations (i.e. law enforcement) regularly seek and gain access to the kind of information we are seeking here. This is not a novel practice.

The Test to be Followed

A person who becomes involved in the tortious/wrongful acts of another has a duty to disclose the identity of the wrongdoer. ISPs are under a duty to do so here. In *Norwich Pharmacal*, [1973] 3 WLR 164 (H.L.), a patent infringement case before the English House of Lords, the Lords found that the defendant patent commissioners were required to assist the patent holders by disclosing the names and addresses of alleged infringing importers. In *Glaxo Wellcome* v. *Minister of National Revenue*, (1998) 81 C.P.R. (3d) 372 (F.C.A.), the Federal Court of Appeal adopted the Norwich principles in deciding that Revenue Canada was required to identify importers of patent infringing chemicals to the Canadian patent holders. The four Norwich principles are as follows:

1. The claim must be *bona fide*.
2. There must be a relationship between the parties, i.e. not mere witness or disinterested bystander, the person must be in some way involved with the wrongdoing.
3. The person from whom discovery is sought must be the only practical source of information available to the appellants.
4. Presumptive obligation to disclose "unless there is some consideration of public policy" mitigating against disclosure.

von Finckenstein J: Are you proceeding under rule 233, 238 or an equitable bill of discovery? [**Ed.:** The order only mentioned the rules, but the argument on the test was the equitable bill].

Dimock, R.: The equitable bill is an underlying duty which can be applied to r. 233 and 238.

(Turning to the test) In *Glaxo*, Stone J. tied *bona fide* to 'frivolous'. We need to prove only an arguable case and that it is not frivolous or vexatious.

von Finckenstein J: I haven't seen any evidence as to why you didn't seek disclosure from KaZaa.

Dimock, R.: I cross examined Shrimpton (Telus technical support) yesterday and his testimony related only to KaZaa Plus (a subscription-based service of KaZaa). We can't get the evidence from KaZaa.

von Finckenstein J: Isn't it up to you to establish that?

Watson, Joel (counsel for Telus)**:** Rather than paraphrasing Shrimpton's evidence, take us to it in the affidavit. The precondition to seeking relief is that the plaintiff must take us to the evidence.

von Finckenstein J: Yes, take us to the affidavit.

Dimock, R.: I will at the appropriate juncture. [**Ed.:** Dimock then briefly discussed – and dismissed – the public policy override as the final Norwich principle]

(Turning to *Straka* v. *Humber River Regional Hospital*, (2000) 51 O.R. (3d) 1). We are not seeking full information, but the bill of discovery does provide for it (at para. 45)

> "It should be noted that disclosure of the wrongdoer's identity is not enough; the obligation extends to giving full information."

[**Ed.:** Referred to the Norwich principle article as saying that although Norwich and Glaxo dealt with patent infringement, the principles can be extended to other situations. *See* K. LaRoche & G.J. Pratte, "The Norwich Pharmacal Principle and Its Utility in Intellectual Property Litigation" (2001) 24 Advocates Quarterly 301 at 311.

Rule 233 deals with documents, while r. 238 allows for third party exam for discovery. It can be done orally or in writing (questions or affidavits). This motion seeks to have an affidavit provided by the respondent ISPs, as the least burdensome method [**Ed.:** Rogers and Bell later argued that affidavits would not be the least burdensome method]

We submit that the ISPs do have this information. We tried to seek it through an informal process, but the ISPs would have none of it, which led us here today. It would be unfair to not allow the plaintiff's discovery here. I'll deal with the expense issue later.

The principle of the duty to identify the wrongdoer can be invoked in this court in a John Doe action or in another action against the third party ISP by way of bill of discovery. It's a matter of process, but the same duty applies.

This motion is not a novel proceeding, contrary to the submissions of some of the ISPs.

Irwin Toy, [2000] O.J. No. 3318 (Sup. Ct.) was brought pursuant to Ontario Rules 30.10 and 31.10 but I would submit that they correspond to federal rules 233 and 238. These rules allow for discovery of documents and information, such as what the ISPs are in possession of and we seek here. *Irwin Toy* dealt with defamation, but the principles also apply here.

CIPPIC makes the argument that this motion is analogous to the high threshold to be met in an application for Anton Piller orders, but we don't think it's the same thing. This is an interlocutory injunction and all we need to show is a prima facie case. The ISPs/interveners have not raised any issues that would militate against this.

[10:42 A.M., court took a short recess]

Dimock, R: I'm going to deal with privacy, which the interveners have raised.

First, this is purely a private matter and the *Charter* does not apply. In *Hill* v. *Church of Scientology of Toronto*, [1995] 2 S.C.R. 1130, the Supreme Court found that private parties do not owe each other constitutional obligations unless the common law is inconsistent with *Charter* values. In *R.* v. *Fegan*, 13 O.R. (3d) 88 (C.A.) the court found:

> While it is unnecessary to dispose of this appeal, I must say that I find offensive the concept that a person who is misusing his telephone to invade, in a most intrusive way, the privacy of other subscribers to the same utility service can set up his constitutional right to privacy as a bar to the efforts of the utility to identify him. As the evidence discloses, there are contractual provisions between Bell Canada and all its subscribers prohibiting just this type of activity, and I would find it most strange if a party in wilful breach of his contract could successfully invoke the protection of s. 8 of the *Charter* to challenge his identification by the utility. To consider the actions of Bell Canada in this instance as being subject to Charter limitations would result, to borrow from the language of Krever J.A. in a similar context in *R.* v. *Shafie* (1989), 47 C.C.C. (3d) 27 at p. 34, 68 C.R. (3d) 259 (C.A.), "in the judicialization of private relationships beyond the point that society would tolerate". On the same theme, La Forest J., in *McKinney* v. *University of Guelph* , [1990] 3 S.C.R. 229 at pp. 262-63, 2 C.R.R. (2d) 1, stated:
>
> > To open up all private and public action to judicial review could strangle the operation of society and, as put by counsel for the universities, "diminish the area of freedom within which individuals can act". In Re *Bhindi* and *British Columbia Projectionists* (1986), 29 D.L.R. (4th) 47, Nemetz C.J., speaking for the majority of the British Columbia Court of Appeal, made it clear that such an approach could seriously interfere with freedom of contract. It would mean reopening whole areas of settled law in several domains. For example, as has been stated: "In cases involving arrests, detentions, searches and the like, to apply the Charter to purely private action would be tantamount to setting up an alternative tort system".

[**Ed.:** *But see Dagenais* v. *CBC*, [1994] 3 S.C.R. 835 "Discretion conferred by a common law rule must be exercised within the boundaries set by the *Charter*; exceeding these boundaries results in a reversible error of law. The traditional common law rule governing publication bans – that there be a real and substantial risk of interference with

the right to a fair trial – emphasized the right to a fair trial over the free expression interests of those affected by the ban and, in the context of post-*Charter* Canadian society, does not provide sufficient protection for freedom of expression. When two protected rights come into conflict, *Charter* principles require a balance to be achieved that fully respects the importance of both rights. A hierarchical approach to rights must be avoided, both when interpreting the Charter and when developing the common law. The common law rule governing publication bans must thus be reformulated in a manner that reflects the principles of the *Charter* and, in particular, the equal status given by the *Charter* to ss. 2(b) and 11(d)."]

Dimock, R.: Turning to PIPEDA, it is clear that an organization can disclose personal information in the event of compliance with the order of a court, etc. (s. 7.3(c)). ISPs do need not obtain consent or even give notice to disclose the personal information of their subscribers pursuant to a court order. The federal Privacy Commissioner has concluded this in several instances, which I won't go into here, save for one: decision #96, which interprets the s. 7.3(c) exception in this manner.

The ISP terms of service (referring to Telus user agreement) prohibits users from engaging in, *inter alia*, copyright infringement. It's the same with Shaw's user agreement. Users have no expectation of privacy with regards to activity which is in breach of their ISPs user agreement, particularly if it is unlawful.

My last point on privacy. The test set here – as suggested by CIPPIC – will not have precedential implications. I want to refer specifically to paragraph 21 of CIPPIC's memorandum. [**Ed.:** Dimock made big hay of this paragraph as suggesting that CIPPIC agreed that the plaintiff's only needed to put forth more than mere allegations. When read in context, this was not suggested.] We are not simply putting forth *mere allegations*, we have evidence.

In passing reference to the privilege argument in the EFC submission, I am not aware of any case which treats the relationship between ISPs and their subscribers as privileged.

Copyright Arguments

Stratton, Bruce: (Gave brief explanation of how KaZaa works)

von Finckenstein J.: Do requests for files go from the requesting peer to the receiving peer directly or is there an intermediary?

Stratton, B.: It is direct. [**Ed.:** If it is direct, then no 'uploading' is occurring, *see R.* v. *McNiven*, [1943 81 C.C.C. 166 (Sask. K.B.) citing *Marino & Yipp* v. *The King*, [1931], 4 D.L.R. 530 (S.C.C.), *R. v. Pecciarich*, (1995) 22 O.R. 3rd, 748, *R. v. J.P.M*, [1996] N.S.J. No. 124 (N.S.C.A.).]

von Finckenstein J.: What does KaZaa provide other than the software?

Stratton, B.: The client software and advertisements, etc.

A KaZaa user has to do multiple things in order to "make available" the protected works, i.e. install the client application, place files in a shared directory, etc. (*see* para. 27 of Millin affidavit, discussing that a copy of a sound file is created). [**Ed.:** The problem with the placement argument is that the act of downloading is the same act as placing the files in the shared folder and downloading is legal. Moreover, if you are ripping songs from CDs this too is legal under s. 80 and yet a later installation of a KaZaa-type application may search for and share these music file formats by default, without the user's knowledge.]

von Finckenstein J.: I understand the process, but this is on the assumption that the user has not blocked the shared files.

Stratton, B.: Evidence shows that all of the 29 shared files in this case. [**Ed.:** But the record doesn't show that there is even a presumption of infringement – Millin can't even differentiate dummy files from real ones and, as far as we know, he didn't even try to ascertain this. Besides, there is no 'making available' right in Canada. To establish infringement, the plaintiffs will need to prove distribution, communication to the public, or reproduction for the *purpose* of trade.]

Stratton, B.: I don't know what the evidence is about what KaZaa knows about the pseudonyms.

von Finckenstein J.: What does a pseudonym actually identify, i.e. does it identify the individual for the purpose of 'uploading' and 'downloading'?

Stratton, B.: (referring to the Millin cross-examination, para. 90) We cannot use pseudonyms for the information that we are seeking in this motion. There is no public source for the information we are seeking. [**Ed.:** But you haven't even attempted to ascertain information from KaZaa, a party with a less remote relationship to the defendants given the third Norwich principle.]

Stratton, B.: (referring to Shrimpton affidavit, para. 14) This is the only evidence on the record suggesting that the information sought here is available else, but it only refers to KaZaa Plus.

Stratton, B: (Went through a sometimes tortured explanation of the KaZaa client, at one point suggesting – in response to a question from the judge – that you could search for all a user's files by typing in the username assigned to that user.) [**Ed.** This is technically incorrect.]

Dimock, R.: I just want to make a correction; apparently, two of the 29 were using iMesh and not KaZaa.

von Finckenstein J: I am quite concerned about the fact that there was no evidence on the record to explain how the KaZaa usernames were connected to a given IP.

Stratton, B.: The ISPs have the information to connect the IPs associated with KaZaa usernames to individuals and they have done this before in response to other types of requests (referred to the Pultz cross-examination which suggests that Shaw does this regularly for other organizations).

Scott, C. (objecting): I would like counsel to refer to more in-depth answers that were provided as supplements to the Pultz cross-examination, specifically questions #4 and #5.

> *Question #5:* The Cable Modem Termination System (CMTS) technologies in use by Shaw and used by Shaw in the past do not log or retain information relating cable modem serial numbers and DHCP information (including IP address and MAC address of Internet device acting as a DHCP client) beyond a real-time basis in volatile memory. Information relating cable modem serial numbers, IP addresses and MAC addresses of Internet devices is available in a real-time basis, and some CMTS technologies will maintain this information for short periods following an Internet device becoming inactive. Some CMTS technologies maintain real-time information regarding cable modems, IP addresses, and MAC addresses which may provide information on cable modem serial numbers, IP addresses, and MAC addresses accurate for approximately the last 24 hours (one half of the standard DHCP lease period). The CMTS devices currently have no capability for logging of historical data relating to cable modem serial, IP address and MAC address for any of the CMTS technologies in use by Shaw. As a result, the CMTS devices used by Shaw provide no reliable way, even from on-line inquiries, to determine an historical association of an IP Address to a cable modem serial number.

[**Ed.:** In plain language, Shaw may be able to respond to realtime requests, but not to ones seeking historical data because it's simply not there.]

Stratton, B.: There is an attack on the ownership of the copyrights [**Ed.:** Typically in copyright infringement cases, the owners submit registration certificates or other proof of ownership, the plaintiffs did not do so here].

Stratton, B.: (Referring to *Lumonic Research* v. *Gould et al*., (1983) 70 C.P.R. (2d) 11 (F.C.A.)) The evidence is that there is no authorization for the exclusive right of reproduction to copy of a sound file into the shared directory.

von Finckenstein J: What about CIPPIC's submission that took issue for that?

Stratton, B.: That's a s. 80 issue. There is a purpose requirement: it must be for private use only and it's hard to imagine a more public place than a shared directory on a computer. To put something on the Internet, is the complete obverse of private. [**Ed.:** This is a flawed argument. Since there is no "making available" right in Canada, placing

something in a shared folder does not authorize its unlawful use. *CCH* v. *LSUC* overturns the Copyright Board's interpretation of authorization on this point. Also, the lack of an intermediary in the shared folder example contrasts starkly with cases of Internet-based distribution in which a work is first uploaded to a third-party (in fact, it is this first act which would be the initial infringement).]

Stratton, B.: Section 80(2) encloses a limitation on use, such as where the purpose is for trade.

von Finckenstein J: What about communication to the public or distribution?

Stratton, B.: By using file-sharing applications, you are engaging in communication. [**Ed.:** This argument is also flawed. There is no practicable way to "send" a file, by request or otherwise, from within a P2P application to another, rather you can only request files using P2P programs at issue in this case.]

Stratton, B.: I refer the court to the definition of authorization "sanction, approve and countenance" in the recent Supreme Court case of *CCH* v. *LSUC*. I would also refer to Tariff 22 (Copyright Bd.), which states that by providing the equipment a user could be deemed to authorize. [**Ed.:** This is clearly inconsistent with *CCH* v. *LSUC*.]

[Court recessed for lunch break, returning at 1:30 PM]

[**Ed.:** Plaintiffs took an hour longer than they had asked for to get through their submission, so the issue of timing came up after lunch. CIPPIC requested an hour and the judge suggested that CIPPIC should only deal with the issues that spoke for the unnamed defendants and that the ISPs could deal with copyright. He suggested this case was not a seminal one and that it was merely about a motion for discovery.]

Dimock, R.: (Dealing with the particulars of the order sought) The plaintiffs seek to examine on affidavit and not to have to call witnesses – we are seeking to simplify the process.

SHAW

Scott, Charles: The information being sought is *prima facie* protected by contract, statute and public policy. In the extraordinary situation, if the court is going to order disclosure, than it should do so only if it is consonant with the rules of court. The court should first ask several key questions: whether a strong case has been made; whether the underlying case is strong; whether the information obtained by this extraordinary process will be reliable and not speculative; and, if an order is to be made, it should be limited in scope to that which the supplier of the information can supply reliablely. The information must not be speculative; it must be conclusive; and, the supplier should be indemnified for all costs and liabilities. This case does not meet those criteria.

I have three points to make.

1. Are there policy, statutory and contractual constraints?

There is no disagreement that the information sought is not personal and as such required by statute and otherwise to be protected. The *ex parte* nature of this motion heightens the test, since the defendants cannot be here to defend their interests.

von Finckenstein J: Why is the proclivity/probability of settlement a concern?

Scott, C.: The plaintiff's parent organization, the RIAA, has threatened users in the U.S. with high-cost litigation and then offered to "settle" for much less. This isn't justice.

This is a 'fishing expedition'. The PIPEDA exemption earlier referred to is for a court order for the purposes of the court, not for the purposes of the plaintiff. The Shaw terms of service place great importance on the privacy of its customers. Our users entered into the contract on that basis. *Charter* values are implicated; the common law is informed by *Charter* values.

The plaintiffs' suggestion that there is a duty to disclose is incorrect. There is no duty. On the contrary we have a duty to protect: under the statute, under the contract and for matters of public policy.

There is an overriding principle for the protection of personal information.

2. The court should only act in the clearest of cases

The plaintiffs should be put to a strict test. They are asking for an extraordinary remedy and they must meet it as follows.

1. Does the case conform to the rules of the court?
    a. You have been asked to address rule 233, but this case does not meet the test set out in the rule, which is limited in scope. Rule 233 only permits the production of documents, it doesn't include analysis, thought, stringing together of didactive reasons, it must be compellable at the trial to this action, not some other action.
    b. At the most rudimentary analysis, this motion does not conform to r. 233.
    c. Regarding, r. 238, paragraph "j" in the plaintiff's notice of motion makes clear that the plaintiffs intend to bring separate actions. They want this information for all proceedings against alleged infringers, not just in this case. What about implied undertakings?
    d. Rules 233 and 238 were never intended to operate as "civil search warrants". The concept of seeking disclosure against one defendant in order to sue another is raised in the equitable bill line of cases, and the plaintiffs try to borrow some of those concepts, but that is not the application before you today. [**Ed.:** This is one of the more confusing

aspects of the equitable bill jurisprudence. Although *Glaxo*, at para. 58, specifically rejects

   e. In the *Norwich* and *Glaxo* cases everyone knew the documents were there – that they existed – but this is a fishing expedition for "documents" that don't even exist.

2. The court ought to consider other relevant practices and principles
   a. implied undertaking rule – information produced by third parties in discovery cannot be used against them in other actions
   b. should not be able to get around the Charter principles
   c. the plaintiffs should not be able to get around statutorily, constitutionally or contractual provisions for privacy
   d. plaintiffs have not done all they could to seek disclosure from more appropriate parties, i.e. KaZaa
   e. they have failed to make more than a speculative case
   f. MediaSentry didn't even listen to the files they identified as infringing – they couldn't even tell whether the files were MediaSentry's own dummy files

von Finckenstein J: What evidence existed that Geekboy had shared files?

Scott, C.: The only evidence of any uploading or downloading that Geekboy did was through MediaSentry.

Geekboy might not even be aware that his files were being shared, that he was even making his files available to others. KaZaa installs to share by default.

MediaSentry themselves admitted that simply knowing an IP address does not lead you to an single computer – it could lead to a residential router, a business, a university or a cybercafé, etc. behind which are many – even hundreds – of computers.

von Finckenstein J: But it will lead to an account holder?

Scott C: But that account holder could be the University of Toronto or Joe Cybercafe or even a purloined account, as through an open wi-fi connection [**Ed.:** Why is this purloined? What about the commons?]

von Finckenstein J: Let's deal with legitimate use.

Scott, C.: I shouldn't be responsible for the actions of my KaZaa-using 21-yr old daughter.

von Finckenstein J: Let's hear about the law.

Scott C.: In my submission, I should not be responsible merely by being the holder of the account. [**Ed.:** *CCH* stands for the proposition that merely providing the equipment does not authorize infringement. There is a presumption of lawful use.]

von Finckenstein J: Shaw must be worried about viruses. They must keep some historical information in order to track virus dissemination?

Scott, C.: Some information is kept, but none of the information that is kept is reliable enough for the purposes that the plaintiffs request it for.

3. Any order given should be limited to the production of existing records and should not require Shaw to swear to what they cannot swear to.

The Pultz affidavit said that Shaw could not provide this information. He distinguished the equitable bill line of cases on the grounds that they sought documents which were already extant.

[**Ed.:** CIPPIC passed Scott the *CCH* reference and he referred to it. von Finckenstein J. made the point that *CCH* also stood for the proposition that control would satisfy authorization, but Scott countered that if his honour knew a way to control 21-yr old daughters then they should have a private conversation.]

TELUS

Watson, Joel: Telus is not here to speak for Internet users, but nor are we here to be conscripted by the CRIA.

The plaintiffs have misinterpreted r. 233; this case is very different from the facts in *Norwich* and *Glaxo*.

They've forgotten about Old Peter Beswick and the third party beneficiary rule! Plaintiffs, as third parties, cannot benefit from the contractual relations of the ISP and its subscribers. The users must be involved and they are not.

von Finckenstein J: In fairness to the plaintiffs, they are asking for the account holder, not the infringer.

Watson, J.: No, (referring to the plaintiff's proposed order as it pertains to Telus) they are asking us to identify sweetydee11@kazaa, who is specifically the alleged infringer and may or may not be the account holder.

von Finckenstein J: But an IP address is like a municipal address.

Watson, J.: The plaintiffs haven't explained this to you. It is not like a municipal address. An IP does not belong to a particular user, it is assigned to him temporarily.

von Finckenstein J: I'm having a lot of trouble with this.

[Watson and von Finckenstein went through a discussion to try and clarify**]**

Watson, J.: The databases that hold the MAC address, the IP address and the billing information for the account holder are not contiguous. It must be generated by deductive reasoning and is expensive.

This case is different from *Norwich* and *Glaxo*, because in those cases the question was "Ought they produce the records?" not "Ought they create the records for a third party."

Telus is not in the business to serve CRIA. This type of civil search warrant is supposed to be an extraordinary remedy. Moreover, they have promised – in their press release – that this is only the "first wave" of several.

von Finckenstein J: But what about their IP rights? (Interested in the equity issue)

Watson, J.: There is a balancing test in *Norwich* and *Glaxo* which limits the disclosure obligations from mere witnesses. We are a mere witness. *CCH* stands for the proposition that merely providing the equipment does not authorize or implicate the intermediary in infringement. PIPEDA would say you have a statutory obligation not to look. Should a mere witness be forced to produce the information? The answer is no.

Rule 233 is for the production of a document. The document must exist already, it is not a "make work" project.

von Finckenstein J: What if the document can be generated by the computer?

Watson, J.: Documents are final work product (He then went into detail on how these documents must be generated by Telus). In *Norwich* and *Glaxo* the respondents had handed over all of the documents, but the names. What the plaintiffs are asking for is to use our mental prowess to correlate the information in our possession into a document they can use.

von Finckenstein J: So it is the correlation that takes you outside the definition of "document".

Watson, J.: We don't have records in our computers at Telus relating to sweetyd11@kazaa

von Finckenstein J: You do now. (Much laughter)

Watson, J: We do. (referring to the motion record itself)

Watson, J.: (Referring to the Millin cross examintation) CRIA has put forth insufficient evidence to support their motion. (Referring to Shrimpton affidavit) We have made the onerous burden of conducting these searches clear to the court. [**Ed.:** Shrimpton testified that Telus staff have no day-to-day knowledge of the MAC or IP address of a given user

even in the event of technical support problems, because they do not use this information for any business purpose.]

Even were r. 233 to apply, Telus staff wouldn't be able to be cross examined on this information, because they do not have knowledge of IP or MAC addresses without investigation. That is not what r. 233 stands for.

The probative value of the information we could produce is limited. Thus, this fishing expedition is putting Telus to a lot of trouble for information that might not even be useful for resolving CRIA's problems.

There is no certainty that CRIA even has the correct information to initiate a search to start with, as they didn't provide any way to test the accuracy of the connection between the KaZaa username and an IP address.

von Finckenstein J: Did you cross examine on this point?

Watson, J.: No, I didn't, but the onus is on them.

von Finckenstein J: Yes, I know. I just wanted to ask since you had raised the point.

Watson, J.: (Started to go through several examples of why identification of the infringer would be very difficult, including open wi-fi hotspots, etc)

von Finckenstein J: But surely I don't need to deal with the identity issues now, but at trial.

Watson, J.: Respectfully, yes you do. What we are being asked to produce is the identification. Once we do this, the identification issue is out of our hands and in CRIA's. At the end of the day, if there is a problem with the identification, Telus will be the one that wears it with their customer base. [**Ed.:** The identification issue also goes to the test.]

von Finckenstein J: And in your submission the identification would not be accurate?

Watson, J.: No.

Watson, J.: KaZaa has much more information than we do about this question.

von Finckenstein J: But you guys carry the traffic between the user and KaZaa, why are you not a party to the communication? Why are you not involved? [**Ed.:** I don't think Watson should even have gone down this road. *Glaxo* at para. 58 "The non-existence of a practical alternative source of information is not in itself a sufficient basis for granting an equitable bill of discovery."]

Watson, J.: There was no question of the patent infringement in *Norwich*. The records had already been produced, etc.

von Finckenstein J: You've done an exemplary job of distinguishing the facts of *Norwich* and *Glaxo* from the facts in this case. Don't flog a dead horse.

ROGERS

Flaherty, Patrick: I have three points.

First, the order sought is exceptional. I'm not going to go into evidence. You've heard these arguments.

Second, the order – if granted – must be more restrictive than what CRIA seeks. It should only require the name of the account holder (not a determination of the infringer) and last known address.

Third, we want costs.

Rogers has two data sets: online data (data from last thirty days). After 30 days it gets archived on tapes for up to 90 days. All the data that is subject to CRIA is archived.

von Finckenstein J: What about all the correlation problems between the MAC address and the IP address?

Flaherty, P.: Apparently, we don't have those problems.

This is a novel case and we must consider it as such.

CRIA should only get the name and last address. That's all they need.

I would like to refer to r. 240(b) – a party on discovery need only disclose the name and last known address. It's not perfectly analogous to the situation here because we are not parties, but it does inform the consideration.

You have jurisdiction under PIPEDA to make an order for disclosure [**Ed.:** This point illustrates the divergence between the ISPs, as it was contrary to what Shaw argued], but the interaction between PIPEDA and the rules is informative on at least two points:

- what would the reasonable person would consider appropriate (s. 3) and
- limited to information necessary for the purpose for disclosure (derived from cl. 4.2.2. limitation exception)

A r. 233 is appropriate here, because Rogers actually has the documents in question. Affidavits, in this case are not the least burdensome method.

To address timing, I would like to ask for 10 days. This case has attracted some profile and your decision will have some precedential value. We need more time to process these

requests. [**Ed.:** I wasn't clear on why the timing issue was related to the public profile of the case]

My last point is related to costs. The Ho (Rogers tech support) affidavit included costs. These aren't manufactured costs, they are representative of what Rogers charges its own companies.

(Addressing the plaintiffs' ISP search chart) This figure of one search a month for the past two years are more or less done in real time (within a week actually) and by government agencies, not private litigants seeking information three months down the road. There is a difference.

BELL

Hodgson, James: Bell does not condone or encourage the use of its service for unlawful purposes. At the same time we are committed to respecting the legitimate assumption that PIPEDA applies. We are all proceeding on the assumption that it does and it would be helpful if this court could make that determination.

Bell is in the unique position among the ISPs to be able to identify all the individuals responsive to CRIA's request. I don't know why this is, but speculate it is due to our 'superior' technology (much laughter)

If the plaintiffs want the evidence in affidavit form, they should pay for it.

Also, Bell should be awarded costs in this proceeding regardless of outcome. That may seem harsh, but they should have picked one user instead of five (as applied to Bell). They chose to have a large action to maximize its deterrent value to other users. I understand why they want to do this, but Bell should not be on the hook for the CRIA's publicity campaign. This is a very expensive (looking around the room at the dozen or more lawyers) way to proceed.

Electronic Frontiers Canada

van der Woerd, David: EFC will adopt the privacy and copyright positions of CIPPIC and the threshold test as outlined by Shaw.

EFC will only address the issue of 'due process'. We are concerned that the *ex parte* nature of this motion precludes participation of the defendants in their own defence. EFC suggests that there is no reason why the court could not address the order to disclose to the defendants directly under r. 238(3)(b). The court could serve the notice on the unnamed defendants instead of on the ISPs. [**Ed.:** This argument was not reflected in their factum and is quite odd. How would the court serve notice on persons it has no knowledge of?]

van der Woerd, D.: Service requirements haven't been met and therefore the requirements of r. 238 haven't been met.

von Finckenstein J: Do you have an analogue for this double-blind procedure?

van der Woerd, D.: I wasn't able to find any authorities.

As a last comment, I would adopt Rogers' argument that the information disclosed should be limited to only name and last address.

[**Ed.:** We live in a society which respects the principle that everyone should have their day in court and that the judicial process should be transparent. While EFC's argument might sound reasonable on its face, in practice it would place the onus on the defendant to appear and defend themselves instead of on the plaintiff to meet a high threshold test. It would likely prove to be more onerous for the unnamed defendants than any of the alternatives argued by CIPPIC or the respondent ISPs.]

von Finckenstein J: We're going to bump CIPPIC to Monday.

Plaintiffs' Reply to Respondents and Intervener EFC

Dimock, R.: Addressed the joinder argument made by Scott and suggested that joinder of parties in cases like is common [**Ed.:** Scott had earlier suggested that joinder would be inappropriate in this case, because the facts of every individual's case would be different. A recent U.S. court found the same, but the statutory regime differs significantly there and may not be applicable. Moreover, splitting these cases up would not necessarily help defendants, because although it would be more expensive for the plaintiffs to prosecute, it would also be more expensive for groups like CIPPIC to oppose and CRIA has deeper pockets than the CIPPICs of the world.]

Dimock, R.: Rule 222 (definition of a document includes…)

Practical source criteria, cited *Alberta Treasury Bd.* **[Ed.:** As far as I know, this case was not on the record] as standing for the proposition that the test of practicability was lowered to one of efficacy.

(Turning to the terms of the order) It's not just the name and address; *Norwich* and the cases that followed stand for the proposition that full information is warranted.

Defendant may hide their tracks. I don't want to draw any negative inferences of the 29 but delivery of affidavit could take time, but in the case of the documents [**Ed.:** This comment suggests that an Anton Piller order for seizure of a filesharer's computer could immediately follow any successful motion to disclose their identity.]

Indemnification of ISPs for misidentification is beyond the pale. There is no precedent for it in equity or elsewhere.

von Finckenstein J: This is an important case.

[court adjourned until Monday at 3 P.M.]

Day 2, March 15, 2004, Ottawa

CIPPIC

Knopf, Howard: CRIA and its members have embarked upon a war against file sharing. In their view, KaZaA and other similar technologies are weapons of mass distribution.

If this motion succeeds, there will be significant collateral damage in this "shock and awe" campaign, as it has been called in the USA, beginning with the 29 defendants in this action. These folks are clearly civilians, they are not commercial pirates. They are, at most, even if you consider all of the inadequate hearsay evidence in front of you today, only the possible account holders of IP addresses that may be been used by somebody but not necessarily the defendant, for file sharing purposes involving only the plaintiffs' agent, and that's assuming that they got the right IP address and it can be correctly traced. A lot of assumptions here… this is not the stuff of which strong *prima facie* cases are made….

These defendants are just 29 of hundreds of millions of P2P users around the world whom the plaintiff' s think are doing something wrong and who could end up being liable in Canada for statutory minimum damages of hundreds of thousands of dollars or more for common everyday behaviour that the plaintiffs had done very little about for years. Unless your last name is Bronfman, potential damages like these will make settlement virtually certain.

Finckenstein J: Please address the four points I gave you in my order to you.

Knopf, H.: CIPPIC will address the following:

1) the test to be applied
2) due process for unnamed defendants, with a suggestion of a creative solution that will protect their interests if this court orders disclosure of their names
3) Privacy rights of defendants
4) Whether there is *prima facie* case of copyright infringement?

Mr. Cameron will take about 15 minutes or so to deal with the first three points and I will deal with the copyright issues.

Cameron, Alex: CIPPIC endorses the position of Shaw on the test, which largely adopted CIPPIC' s written submissions, paras. 22-39 of our memorandum. I will be dealing with four issues today, as follows:

1. Privacy and the application of the *Charter*
2. R.E.P. and the invasiveness of the order sought.
3. Harm to public interest if order granted.
4. Nature of test, if order granted.

The plaintiffs argue that this is not a novel case. With all due respect, this is a novel case. The facts are new and have never been dealt with before, the very cause of action is being challenged, plaintiffs' evidence has been challenged, and the scope of r. 233 is being challenged. It is also novel because it involves 29 defendants, and many others will follow.

On Friday, the court heard submissions from Shaw and Telus to the effect that Rules 233 and 238 have no application to this case. The Court also heard arguments that the *Norwich* line of cases don' t apply and are distinguishable from in the present case. CIPPIC adopts those submissions.

CIPPIC also notes that the court in *Glaxo*, at para. 62, was skeptical about whether the identity information at issue there was confidential or sensitive because it would have passed through many hands before reaching customs officials. Moreover, the information sought in the *Norwich* and *Glaxo* cases was sought for a regulatory purpose precisely to be disclosed. That is clearly not the case here where, as I will submit, the information at stake is highly private and sensitive and not collected for a regulatory purpose. The SCC has clearly stated that information collected for a regulatory purpose is subject to a lower expectation of privacy than other types of information. *R.* v. *Fitzpatrick* [1995] 4 S.C.R. 154 at para. 49.

<u>Privacy and the applications of the Charter</u>

There is no dispute that the common law in this case must be interpreted in a manner consistent with *Charter* values. That alone requires the court to be mindful of the *Charter* protection of a reasonable expectation of privacy in making the order in this case.

However, the plaintiffs have alleged that the *Charter* does not apply in this case because it is civil in nature (para 47-48).

(Referring to *Dagenais* v. *CBC*, [1994] 3 S.C.R. 835) This is a case involving a *Charter* challenge to the common law rule allowing a court to impose a publication ban.

> As the *Constitution* is the supreme law of Canada and any law that is inconsistent with its provisions is, to the extent of the inconsistency, of no force or effect, it is impossible to interpret legislation conferring discretion as conferring a power to infringe the *Charter*, unless, of course, that power is expressly conferred or necessarily implied. Such an interpretation would require us to declare the legislation to be of no force or effect, unless it could be justified under s. 1.

> I would extend this reasoning, and hold that a common law rule conferring discretion cannot confer the power to infringe the *Charter*. Discretion must be exercised within the boundaries set by the principles of the *Charter*; exceeding these boundaries results in a reversible error of law. In this case, then, we are dealing with an error of law challenge to a publication ban imposed under a common law discretionary rule.

The *Federal Court Act* and Rules are the legislation conferring the discretion on this court to grant the order sought and so the *Dagenais* reasoning is directly applicable. In this case, this means that the court must exercise its discretion in compliance with the *Charter* rights of any individual affected by the order.

This means, for example, that the order must respect the reasonable expectation of privacy of the ISP account holders which I will come to in just a moment. It also means that, as the Supreme Court recognized in *R.* v. *Dyment*, [1988] 2 S.C.R. 417 at 428 "retention of information about oneself is extremely important" and at 430, "if privacy of the individual is to be protected, we cannot afford to wait to vindicate it only after it has been violated." CIPPIC submits that these kinds of considerations require the Court to impose a high threshold on plaintiffs seeking the kind of order sought in this case.

von Finckenstein J: I guess the upshot is that the court should focus on preventative measures?

Cameron, A.: Exactly.

<u>Reasonable expectation of privacy and the invasiveness of the order sought</u>

The invasiveness of the order sought in this case parallels the invasiveness of Anton Piller orders. In each case, a plaintiff seeks the right to have access to the private premises (or in this case highly private information) of an individual without notice to the individual and prior to the court making a determination regarding the alleged wrongs. Indeed, it is arguable that the present case is even more extreme than an Anton Piller order because the unnamed ISP subscribers have no ability to close the metaphorical door on a plaintiff who comes knocking for access. Even more invasive because the defendants have no ability to close the metaphorical door on plaintiffs who come knocking for access. The harm is permanent. In Anton Piller you can return goods, in *Charter* you can exclude evidence, the def. cannot recover their privacy rights once breached. They will be gone forever.

First, in my experience, Anton Piller orders are typically executed in shopping malls, flea markets and retail stores, not in personal residences. And yet those civil searches nevertheless require a high threshold test.

Second, that in *Hunter* v. *Southam*, [1984] 2 S.C.R. 145, the Supreme Court of Canada has clearly stated that privacy protects people, not places. As I submit is the case here, a violation of informational privacy irrespective of location may be equally or much more

invasive than a search of a personal residence. This is supported also by the *R.* v. *Dyment*, [1988] 2 S.C.R. 417 case which recognizes the importance of informational privacy.

And third, that the *R.* v. *Plant*, [1993] 3 S.C.R. 281 case cited by the plaintiffs actually supports the conclusion that the information sought here is clearly protected by an expectation of privacy and that the search here is very invasive.

(referring to *Plant*) information obtained from third party (para. 41) records are telling of what happens inside a private residence – home is most private of places (para. 45) computers may and should be private places where the information they contain should be subject to a reasonable expectation of privacy

Information at issue here will directly – not by inference as in *Plant* – reveal the activities of individuals on the Internet.

von Finckenstein J: But all I would be ordering is the disclosure of names?

Harm to public interest if order granted

Cameron, A.: At first blush this case appears to merely involve disclosing identities, but in reality it involves much more because of the way that the identities at stake can be linked to people' s otherwise anonymous online activities through IP addresses and peer to peer usernames. This case is unlike any other in the way that the order sought may breach the privacy rights of individuals, causing harm to them and to the public interest.

People who will be affected by the order in this case and future cases are people who very well may have engaged the Internet and peer to peer systems broadly on the assumption that all of their activities were and would remain anonymous. This is important because the Internet and P2P provide an unprecedented forum for freedom of expression. Because that expression is made anonymously, it permits users to communicate unpopular or unconventional ideas without fear of ridicule, harassment or discrimination on, for example, the basis of race, gender, or socio-economic status.

von Finckenstein J: This order would not give access to the defendants' computers. Merely because the identity is disclosed would not lead to wider exposure.

Cameron, A: The plaintiffs' have made the point that they are concerned about the destruction of evidence. It is conceivable that the next order they ask for after disclosure is a real Anton Piller order for the seizure of the defendants' computers.

von Finckenstein J: Not by this order, but by subsequent orders.

Cameron, A.: It is conceivable.

von Finckenstein J: How are these users any different from any other defendants?

Cameron, A.: Internet encourages activity people may not otherwise engage in because it is anonymous.

In addition to these serious harms to individuals, granting the order sought in this case will have more general impacts on the public interest. If granted, the order may have a significant chilling effect on the use of the Internet and innovative file-sharing technology generally, for example, for freedom of expression and freedom of religion. Therefore, these are very much at issue in this case.

There are alternative ways for ways plaintiff to get information, but CIPPIC submits that a lack of an alternative should not be determinative as to whether it is granted. [**Ed.:** This is in reference to para. 58 of *Glaxo.*]

von Finckenstein J: Let me summarize. It is a two stage test: there must be no other source and I must consider the public interest?

Cameron, A: Close.

von Finckenstein J: Put it in your words.

Nature of test, if order granted

Cameron, A:

1. Has the plaintiff made out an extremely strong *prima facie* case?
    a. Is there clearly a cause of action which would apply to the facts as alleged by the plaintiff? The answer is NO and Mr. Knopf will address this.
    b. In the intellectual property context, has the plaintiff clearly demonstrated its rights as well as the alleged infringement? Again, the answer here is NO, the ISPs have described a number of problems with the Plaintiffs evidence, including the fatal fact that there is no evidence that anyone actually listened to the files at issue.
    c. Has the plaintiff made a full and frank disclosure to the court, including the strengths and weaknesses of the plaintiff' s case in fact and law? (*e.g.*, as to whether KaZaA users may be unintentional or inadvertent file-sharers) The answer here is NO – most fatally, Mr. Millen did not explain what was clearly within his power to explain – ie. how he or someone else at his company linked the usernames to the IP addresses.
    d. Has the plaintiff filed affidavits based on personal knowledge of the representatives of the plaintiff? The answer here again is NO. Mr. Scott for Shaw dealt with Mr. Millen's affidavit and the same issue arises in Ms. Yonekura's affidavit which is almost entirely hearsay.
2. Are there alternative ways for the plaintiff to obtain the information sought? (*e.g.* from the file-sharing services directly, as suggested by the Affidavit of David Shrimpton (Telus), at para. 14) This was the subject of much attention at the hearing on Friday. CIPPIC agrees with those submissions which pointed out that

the burden on this point is entirely with the Plaintiff and that Kazaa Plus may be another source. More importantly, however, CIPPIC submits that this factor is NOT determinative. The order should not be granted merely because the information cannot be obtained elsewhere. As in this case, there may well be many cases where plaintiffs will fail to meet other parts of the test suggested here or where the public interest outweighs granting the order sought.

3. What is the harm to the plaintiff if the order is not granted?
4. Will granting the order respect *PIPEDA* and *Charter* rights and values?
5. Will granting the order potentially cause irreparable harm to innocent ISP subscribers?
6. Will the order likely amount to a final determination of the action?
7. Does the plaintiff have clean hands at the time the order is sought?
8. Has the plaintiff provided undertakings regarding damages? While undertakings would be required in Anton Piller cases, more is at stake here and CIPPIC would caution the court against putting very much emphasis on using an undertaking as a safeguard. The harm to individuals here may likely be irreparable and of the kind that money could never repair. Further, individuals may not have the resources to enforce undertakings to trial.

[court recessed for five minutes due to technical difficulties]

Copyright

Knopf, H.: I realize that this motion is unlikely to be the forum for a definitive ruling on whether so-called "uploading" – I don't like the term, but others are using it so I will – is legal in Canada and there is no need for such a ruling. We certainly don't need to consider whether downloading is legal – the Copyright Board has just done that. The Plaintiffs have questioned it in the press, but not in this case. They have publicly and notoriously indicated that they are targeting "egregious uploaders".

We are simply asking this court to rule that the plaintiffs have not met the necessary threshold for the extraordinary relief that they seek. The have several thresholds to satisfy – last but not least being that they have a strong *prima facie* case in terms of copyright law (para. 62 of their memo) and we say that they clearly do not on the wording of the current statute, even if the facts they allege are true and even if you accept their evidence which we say is inadmissible or at best virtually weightless.

I find it interesting that the plaintiffs have slipped back into suggesting that they have an arguable case, but that' s not good enough.

von Finckenstein J: This case turns on the language of *prima facie*.

Knopf, H.: I accept that.

But if the Court does dismiss this motion without even getting to the copyright issues, it would still be very useful to have the Court' s view on whether there is a *prima facie*

copyright infringement case here in order to avoid us having to do this all over again if and when the plaintiffs get their evidentiary ducks in order, or if there is an appeal from your order.

If there is not, then the Plaintiffs will *not be without recourse*. They will have even more ammunition for their already intense lobbying campaign to change the law that they are themselves responsible for, which is the law that makes this P2P activity arguably legal in Canada.

If this was *prima facie* case they would not need a 38 page memo.

von Finckenstein J: Focus on whether they have made out a *prima facie* case.

Knopf, H.: Pardon the expression, your honour, but that is music to my ears.

Copyright law is very precise. It is not, as we'll see, an open ended tort scheme. If there is no explicit right, then there is no explicit remedy. The only remedy is in Parliament and that's where the Plaintiffs need to be on this case, as they were last week and were in 1996 and 1997 when they got Part VIII of the *Copyright Act* – the private copying levies – introduced, which is proving to be a problem for them in certain respects.

I am very pleased that they used the word "non-suited", because that means they acknowledge they have not made out the case on the evidence.

The plaintiffs set out four causes of action:

1) reproduction
2) distribution
3) authorization
4) possession

CIPPIC submits that the plaintiffs' have not made out any claim of copyright infringement in this case, let alone the *extremely strong prima facie case* which is the appropriate test in this type of motion. In particular:

Any reproduction of copyrighted materials that may have been made by the Defendants is legal by virtue of s. 80 of the *Copyright Act*.

Distribution must entail a purposeful, intentional and active sending and receipt. There is no evidence of any illegal distribution by any of the defendants.

Secondary infringement as set forth in s. 27(2) of the *Copyright Act* requires knowledge on the part of the infringer. There is no evidence before the Court sufficient to establish that any of the defendants knew or ought to have known that any activity of the nature alleged has ever taken place, or to establish a potential basis for vicarious liability. There is no "making available" right of copyright holders in Canadian law.

Merely providing equipment or authorizing the use of equipment that could be used for infringement does not amount to infringement. Even if there is infringement, a defendant will not be liable if it lacks sufficient control over the activity.

The plaintiffs have failed to file sufficient evidence to show that any of them are the owners or exclusive licensees of specific copyrights so as to entitle them to succeed in this action.

There is no evidence that uploading is taking place. There is no "making available" right in Canada. Merely providing equipment does not make a parent liable for anything under Canadian law. If that wasn' t clear ten days ago it certainly is now under *CCH*.

von Finckenstein J: You make mention of an international "making available" treaty to which Canada is not a party. Draw the distinction between making available and distribution or communication for me.

Knopf, H.: Making available under WIPO does not require active participation in the way that distribution and communication does.

von Finckenstein J: How do you answer Mr. Dimock, if you put something in a shared folder you implicitly make it available. Aren' t we splitting hairs?

Knopf, H.: The plaintiffs have avoided mentioning "communication to the public" or "transmission" because they know they can' t prove this. It is not up to us to amend the law. If and when the plaintiffs get their WIPO treaties, it may or may not get taken care of.

von Finckenstein J: OK.

Knopf, H.: The plaintiffs argued that the way that KaZaa works implicates the making available right.

von Finckenstein J: How does KaZaa work?

Knopf, H.: The way in which it works has been laid out quite well in the *Grokster* case (*Metro-Goldwyn-Mayer-Studios, Inc. v. Grokster*, 259 F.Supp.2d 1029 (C.D.Cal. 2003), which you have before you. Someone may be making something available unintentionally. KaZaa simply lists music titles and you can' t necessarily tell what the song is from the title.

Sharing file using P2P applications does not require someone to send something to a BBS.

Section 80 requires purpose, which is as close as we can get to *mens rea* (guilty mind) in the civil law.

The product must be the product of primary infringement, i.e. communication or reproduction (referred to Rothstein J.A.'s comments in *CCH* at the Fed. Ct. of Appeal).

He said there must be a sale and I would submit for there to be a sale there must be a recipient.

Finally, s. 27(2)(b) requires that the distribution must be *prejudicial* to the copyright owner. There is no evidence of this. The plaintiffs have not filed any evidence that filesharing affects prejudicially the owner of the copyright.

von Finckenstein J: I can' t take judicial notice?

Knopf, H.: You can take judicial notice of their claims as long as you also take notice of some of the other things I've mentioned. There are studies showing that this activity may increase business for the plaintiffs. I refer in particular to studies by Stan Leibowitz, but there are others.

von Finckenstein J: (taking notes) OK.

Knopf, H.: The authorization right has been clarified in *CCH*. An account holder should not be held liable simply because someone using their account is arguably using the computer unlawfully. We all had a good chuckle the other day at the example Mr. Scott gave of controlling teenage daughters.

von Finckenstein J: Surely we are here to talk about is the *prima facie* test. The account holder is *prima facie* responsible for his account. I don't have to deal with vicarious liability now, do I? Can we consider the account holder *prima facie* responsible for the activities taken by others using the account? Isn't the account holder like the owner of a car, liable for everything that happens with the car?

Knopf, H.: Car owners are liable for some things which happen with their cars, such as parking tickets, but that's because society has decided this. I recall finding an eight volume treatise from the 1930's on the law of the automobile in the Supreme Court of Canada library. Back then automobiles were new technology and the law was in a mess. We recognized that we can't have full scale trials over every parking ticket and so we considerably simplified the law of the automobile through statute and contract: we no longer need eight volume treatises. That's not the case here regarding internet accounts and copyright law. The account holder may be the last person that should be held liable. The plaintiffs are using this as a fishing expedition to discover the alleged culprit.

von Finckenstein J: OK, I hear you.

Knopf, H.: (referring to *CCH*) The SCC has found that someone who merely provides the equipment bears no responsibility unless they are in a position of control.

Getting back more to the general comments. There is an old principle in copyright that technology challenges copyright. Copyright is a limited monopoly conferred by Parliament.

I am not without sympathy for the plaintiffs' conundrum but that sympathy does not extend to the point of the court inferring rights that don' t exist in statute.

The plaintiffs have not provided any evidence of how they got the IP addresses.

No evidence before the court that the plaintiffs own the copyrights. It's a weightless affidavit.

I would be willing to let you admit the Yonekura (CRIA anti-piracy officer) affidavit to get on with the motion so that we can discuss it on the merits and not a technicality.

von Finckenstein J: That is very gracious of you!

Knopf, H.: (turning to the order sought) Turning to *Okanagan*, very few people will be able to afford a proper defence. Consequently, there will be forced settlements on issues that should go to trial.

von Finckenstein J: You can' t have it both ways Mr. Knopf.

Knopf, H.: This is an alternative remedy.

Dismissing this motion would be less drastic than allowing it. Allowing it would change the motion would change the law in Canada forever. The plaintiffs have not adduced any evidence to justify this extraordinary relief.

Proffessor Geist was quoted on Friday as saying:

> *"It's a critical case because it lies at the intersection of so many interesting online issues, both copyright and privacy and the right to anonymity and responsibility of intermediaries, namely the ISPs… all are issues that on their own are significant. This is almost the perfect storm where you bring together all of those issues into a single case."*

I submit that the calm at the centre of this storm relates to the vacuum created by the lack of evidence and a cause of action.

von Finckenstein J: What about the issue of authorization? If someone has an accident with a car or if a car is stolen, the liability falls to the owner of the car.

Knopf, H.: The way these questions have been answered are with statutes.

Plaintiffs' Reply to CIPPIC

von Finckenstein J: (speaking to Dimock, R.) It would help me if you addressed some of the issues raised by Mr. Knopf and others. First, link to IP address and pseudonym. Second, nobody actually listened to the songs and no evidence of "distribution" to anyone but Millin (Mediasentry). Third, deal with the working of KaZaa. Isn' t it passive?

Dimock, R.: (on reply) The argument put forth by Mr. Cameron rested his case principally on the Anton Piller test. No other test, not even the injunction test, requires a higher test than *prima facie* or arguable. If we look at Anton Pillers they are quite invasive, but what we are seeking here are names. The Anton Piller goes much further. It allows one party to enter another's premises, his suitcase. It is far more invasive than anything sought here to remove the anonymity of a copyright infringer.

My friend Mr. Cameron referred to the *Charter* and *Charter* values. *Charter* values cannot apply; we cannot have an over-judicialization of private relationship (referred to *R.* v. *Fegan*, (1993)13 O.R. (3d) 88 (C.A.).

In *Viacom Ha! Holding Co.* v. *Jane Doe*, (2000) 6 C.P.R. (4th) 36) the defendants attacked the Anton Piller order and the court replied that the *Charter* does not apply to private disputes:

> In my view, based on the foregoing, it can be said that when a court order is granted to resolve a private litigation based on the common law, it cannot be a government action to which the *Charter* applies.

The court also found that an Anton Piller is not subject to search and seizure requirements.

> The execution of an Anton Piller order, a process which is civil in nature, is not subject to the search and seizure requirement as set out by the Supreme Court of Canada in Southam, the 'prior authorization based on the existence of reasonable and probable grounds'.

If we seek more invasive remedies we have to come back to this court, right now all we want are identities.

In *Plant*, the decision of McLaughlin J. were additional reasons to those given by the majority, quoting:

> In addition to the fact that the manner and place of the search are indicative of a minimally intrusive search, the seriousness of the offence militates in favour of the conclusion that the requirements of law enforcement outweigh the privacy interest claimed by the appellant.

PIPEDA recognized both privacy rights and exceptions, including compliance with a court order or even less, the rules for production of documents in a court.

The right to remain anonymous was again mentioned by Mr. Cameron and I wonder how this is put in proper perspective when one looks at CIPPIC's own memo at para. 21. "The right to privacy is not absolute. For example, a person does not have the right to anonymously defame, infringe or extort."

There was also reference by Mr. Cameron to the *Irwin Toy* case and I want to address some of the arguments he made in paragraph 10 of that case. Particularly the fact that nobody appeared on behalf of the unnamed defendant or the ISP respondent, as we have here. In such cases, the court will be more cautious because the lawyers are not there to argue it.

Just as Stone J.A. said in *Glaxo*, we only need a *bona fide* case.

I also submit that it would be incorrect to state that the tort of defamation is any more defined than the tort of copyright infringement. The latter has a long history.

Mr. Cameron concluded his remarks by looking at para. 37 of CIPPIC' s memo. I will address those briefly.

1) We do not need a strong prima facie, only a prima facie
2) Information and belief should satisfy in lieu of personal knowledge
3) No alternative ways have been put forward by anyone (Finckenstein : Surely it is up to you?)
4) What is the harm? (to stop the plaintiff now would be to make a determination on the merits)
5) This order would respect PIPEDA and Charter rights and values.
6) No harm will only be damages for copyright infringement.
7) No, this is not a final determination.
8) Yes.
9) Never has this court required undertaking with regards to the production of documents, only with regard to injunctions (Finckenstein : such as Anton Pillers). Right.

Turning now the submissions made by Mr. Knopf (he mistakenly referred to Knopf as having cited *Dagenais*)

Link between the IP address and the customer account (pseudonym). The ISPs can help us with the IP address at that particular time and the customer account.

von Finckenstein J: The question is how is the KaZaa pseudonym related to the IP address given to the ISPs?

Dimock, R.: There is something in the system MediaSentry uses that does this. There is nothing on the record explaining how this is done. Nor did anyone cross-examine Mr. Millen on this question.

Knopf, H.: (objecting) With respect, it is not our job to rehabilitate the plaintiffs' witness.

von Finckenstein J: Can you take me to this or perhaps the ISPs representative can take me to this?

DiPucchio, Rocco: I' m at a disadvantage as I don' t have all my materials.

Knopf, H.: I believe I have the reference.

DiPucchio, R.: For the record we did object to that line of questioning.

Knopf, H.: See paragraph C in Tab C of CIPPIC's motion record (referring to the cross-examination of Gary Millin).

Dimock, R.: Your third question dealt with the sharing of files in a folder and whether that constituted authorization.

The reproduction of any of the thousands of songs into the shared directory meant that Geekboy was, in effect, not making it for his private use, but for the use of others. Section 80 does not apply in those circumstances. He is also authorizing others to infringe. Section 3(1) and s. 27(1) provide that 'authorization' is a "separate protected use under the Act".

Let me clarify the *CCH* case (**Ed.:** Dimock then referred to the *Tariff 22* case (as dealt with by the Copyright Board) and not *CCH* that by making something available you are authorizing it. CCH].

In short answer to Mr. Knopf, this does constitute authorization.

von Finckenstein J: Your key argument is para. 116 of your memo; that is your distinction between CCH and this case.

> "In determining the question of authorization, there is a distinction between the provision of equipment that may or not be used for infringement (no authorization), and the copying of files into a system that is aimed at having others receive copies (authorization)."

Dimock, R.: Yes.

von Finckenstein J: You don' t have to take as long as Mr. Knopf did to make your point (laughter).

Dimock, R.: I will take your advice to Mr. Stratton and quit while I' m ahead, but I have one last point. Referring to para. 38-39 of the *Okanagan* decision cited by CIPPIC in

their authorities, (*British Columbia (Minister of Forests)* v. *Okanagan Indian Band* [2003] S.C.J. No.76).

> The present appeal raises the question of how the principles governing interim costs operate in combination with the special considerations that come into play in cases of public importance. In cases of this nature, as I have indicated above, the more usual purposes of costs awards are often superseded by other policy objectives, notably that of ensuring that ordinary citizens will have access to the courts to determine their constitutional rights and other issues of broad social significance. Furthermore, it is often inherent in the nature of cases of this kind that the issues to be determined are of significance not only to the parties but to the broader community, and as a result the public interest is served by a proper resolution of those issues. In both these respects, public law cases as a class can be distinguished from ordinary civil disputes. They may be viewed as a subcategory where the "special circumstances" that must be present to justify an award of interim costs are related to the public importance of the questions at issue in the case. It is for the trial court to determine in each instance whether a particular case, which might be classified as "special" by its very nature as a public interest case, is special enough to rise to the level where the unusual measure of ordering costs would be appropriate.
>
> One factor to be borne in mind by the court in making this determination is that in a public law case costs will not always be awarded to the successful party if, for example, that party is the government and the opposing party is an individual Charter claimant of limited means. Indeed, as the B. (R.) case demonstrates, it is possible (although still unusual) for costs to be awarded in favour of the unsuccessful party if the court considers that this is necessary to ensure that ordinary citizens will not be deterred from bringing important constitutional arguments before the courts. Concerns about prejudging the issues are therefore attenuated in this context since costs, even if awarded at the end of the proceedings, will not necessarily reflect the outcome on the merits. Another factor to be considered is the extent to which the issues raised are of public importance, and the public interest in bringing those issues before a court.

von Finckenstein J: Make your arguments available to the court electronically. (to Dimock) How would you feel if I deny the order, I deal with the issue of infringement?

Dimock, R.: I don' t think we need to do that.

von Finckenstein J: I will take it under advisement. I realize there is urgency in this case and I will try and have a decision by Friday.