Chapter #

NYMITY, P2P & ISPs

Lessons from BMG Canada Inc. v. John Doe[1]

IAN KERR* and ALEX CAMERON**

**Canada Research Chair in Ethics, Law & Technology, Faculty of Law, University of Ottawa (iankerr@uottawa.ca); **LL.D. (Law & Technology) Candidate, University of Ottawa (acameron@uottawa.ca)*

Abstract: This chapter provides an exploration of the reasons why a Canadian Federal Court refused to compel five Internet service providers to disclose the identities of twenty nine ISP subscribers alleged to have been engaged in P2P file-sharing. The authors argue that there are important lessons to be learned from the decision, particularly in the area of online privacy, including the possibility that the decision may lead to powerful though unintended consequences. At the intersection of digital copyright enforcement and privacy, the Court's decision could have the ironic effect of encouraging more powerful private-sector surveillance of our online activities, which would likely result in a technological backlash by some to ensure that Internet users have even more impenetrable anonymous places to roam. Consequently, the authors encourage the Court to further develop its analysis of how, when and why the compelled disclosure of identity by third party intermediaries should be ordered by including as an element in the analysis a broader-based public interest in privacy.

Key words: Privacy, anonymity, compelled disclosure of identity, Internet service providers, peer-to-peer, copyright, cybercrime

Some people go online to share music – to explore the limits of their imaginations, to sample, to up and download songs from various musical genres and feel the beat of previous generations. In the U.S., sharing music

[1] BMG Canada Inc. v. John Doe, 2004 FC 488, *available at* http://decisions.fct-cf.gc.ca/fct/2004/2004fc488.shtml.

across some peer-to-peer (P2P) networks is illegal.[2] In Canada, it is not.[3] Not yet.[4]

Some people go online to construct nyms – to engage in a social process of self-discovery by testing the plasticity of their identities and the social norms from which they are constituted. In the U.S., this form of personal exploration has been compromised by litigation campaigns that have successfully sought to compel Internet service providers (ISPs) to disclose their customers' offline identities.[5] In Canada, such campaigns have not enjoyed the same success. Not yet.

Why did a Canadian court refuse to compel the disclosure of the identities of twenty nine P2P file-sharers whom the Canadian Recording Industry Association (CRIA) wished to sue for copyright infringement? Ought this decision to be upheld on appeal? What can be learned from this decision?

This chapter aims to address the above questions and to reinforce the motif that we must tread carefully at the intersection between the procedures and policies supporting digital copyright enforcement and online privacy.[6]

[2] A&M Records, Inc. v. Napster, Inc. 239 F.3d 1004 (9th Cir. 2001).

[3] *See* BMG v. Doe, 2004 FC 488.

[4] BMG v. Doe, 2004 FC 488, *appeal filed*, No. A-T-292-04 (F.C.A. Apr. 13, 2004), *available at* http://www.cippic.ca/en/projects-cases/file-sharing-lawsuits/criaappealnotice.pdf.

[5] *See, e.g.*, Keith J Winstein, *MIT Names Student as Alleged Infringer*, The Tech, Sept. 9, 2003, *at* http://www-tech.mit.edu/V123/N38/38riaa.38n.html; John Borland, *RIAA Targets Students in New File-Swapping Suits*, Cnet News.com, Oct. 28, 2004, *at* http://news.com.com/2102-1027_3-5431231.html?tag=st.util.print; *Electronic Frontier Foundation Defends Alleged Filesharer*, Electronic Frontier Foundation, Oct. 14, 2003, *at* http://www.eff.org/IP/P2P/20031014_eff_pr.php; Katie Dean, *RIAA Hits Students Where it Hurts*, Wired News, Apr. 5, 2003, *at* http://www.wired.com/news/digiwood/0,1412,58351,00.html. Not every attempt to compel subscriber identities from ISPs in the United States has proven successful. Some courts have shown that subscriber identities should not be handed over too easily. *See, e.g.*, Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., 2003 U.S. App. LEXIS 25735.

[6] This motif, though it is not novel among legal academic circles, has not yet enjoyed general recognition outside of a relatively small community of experts. *See, e.g.* Michael Geist, *Web Privacy vs. Identifying Infringers*, The Toronto Star, Oct. 6, 2003, *available at* http://www.michaelgeist.ca/resc/html_bkup/oct62003.html; Alex Cameron, *Digital Rights Management: Where Copyright and Privacy Collide*, 2 Canadian Privacy Law Rev. 14 (2004), *available at* http://anonequity.org/files/a_comeron-Where_Copyright_and_Privacy%20Collide.pdf; Alice Kao, *RIAA V. Verizon: Applying the Subpoena Provision of the DMCA*, 19 Berkeley Tech. L.J. 405 (2004); Robert J. Delchin, *Musical Copyright Law: Past, Present and Future of Online Music Distribution*, 22 Cardozo Arts & Ent. L.J. 343 (2004).

1. NYMITY

As many scholars have pointed out, there is little consensus as to whether our ability to disconnect our actions from our identities is, on balance, a good thing.[7] Anonymity is like the Duke's toad – ugly and venomous, and yet it wears a precious jewel in its head.[8]

Ugly and venomous, because it disables accountability and enables wrongdoing. In the P2P context, an inability to ascertain the real-life identities of *geekboy@KaZaA, mr_socks@KaZaA, chickiepoo25@KaZaA*[9] and other file-sharers facilitates their ability to copy and disseminate music *en masse*, carefree and without a trace. Without knowing their identities, CRIA and other such organizations cannot sue these individuals and consequently cannot test the claim that file-sharers are engaging in illegal conduct. This could be a serious problem because, if anonymous P2P networks were undefeatable, copyright industries would have no means of legal recourse. As Lessig once remarked, in its broader context, "[p]erfect anonymity makes perfect crime possible."[10] While illegal copying of MP3s is unlikely to unravel civilization as we know it, a more generalized ability to commit perfect crime might. There are good reasons to fear a society in which people are able to act with impunity. Consequently, there are good reasons to fear anonymous P2P networks.

Though dangerous, anonymity is at the same time precious. It is Plato's *pharmakon;*[11] a drug that is both poison and remedy. As Derrida might have described it: "[t]his charm, this spellbinding virtue, this power of fascination, can be - alternately or simultaneously - beneficent or maleficent."[12] The ability to use "nyms" – alternative identifiers that can encourage social experimentation and role playing – is "an important part of the rich fabric of human culture."[13] Anonymity facilitates the flow of information and communication on public issues, safeguards personal reputation and lends voice to individual speakers who might otherwise be silenced by fear of retribution.[14] Nyms can be used to enhance privacy by controlling the

7 *See, e.g.,* A. Michael Froomkin, *Anonymity in the Balance*, *in* Digital Anonymity and the Law (C. Nicoll et al. eds., 2003). *See generally* G.T. Marx, *What's in a Name? Some Reflections on the Sociology of Anonymity,* 15(2) Info. Soc'y 99, 99-112 (1998).

8 William Shakespeare, *As You Like It,* act 2, sc. 1.

9 These are some of the nyms at issue in BMG v. Doe, 2004 FC 488.

10 L. Lessig, *The Path of Cyberlaw*, 104 Yale L.J. 1743, 1750 (1995). *See also* A. Michael Froomkin, *Anonymity and Its Enmities*, 1995 J. Online L. art. 4 (June 1995), para. 46.

11 J. Derrida, *Plato's Pharmacy*, *in* Dissemination 95 (B. Johnson trans., 1981).

12 *Id.* at 70.

13 Roger Clark, *Famous Nyms* (Aug. 31, 2004), *at* http://www.anu.edu.au/people/Roger.Clarke/DV/FamousNyms.html.

14 Marx, *supra* note 7.

collection, use and disclosure of personal information. Anonymity can also be used to protect people from unnecessary or unwanted intrusions and to "encourage attention to the content of a message or behavior rather than to the nominal characteristics of the messenger."[15]

It is not our aim in this short chapter to resolve the conflicting value sets generated by the possibility of perfect anonymity, nor to make a case for some intermediate solution such as pseudonymous or traceable transactions. Although there are a number of technological applications seeking to create both such states of affairs,[16] the typical uses of online nyms are much more leaky. That is, one nym can usually be associated with another or with other information to create a personal profile that enables identification.

For example, "*geekboy@KaZaA*" is one kind of nym, "24.84.179.98" is another. The latter, sometimes referred to as an IP address, is a numeric identifier assigned to computers or devices on TCP/IP networks. IP addresses are easily discovered and observed as people transact online. The particular IP address referred to above is alleged to belong to the network device used by an individual whose KaZaA pseudonym is *geekboy@KaZaA*.. In the context of the recording industry's campaign against P2P file-sharers, finding out the IP address of this device is currently the best first step in uncovering the identity of an individual file-sharer. But the IP address is not enough. In order to sue, it is necessary to tie the device's IP address to a legal name. This is not always easy to do. Not without help from a third party intermediary. In this case, the ISPs were targeted and will be the focus of discussion in this chapter. However, the information might have been available from any intermediary, including from the operators of KaZaA or other P2P networks.

In our information society, ISPs have increasingly become trusted holders of and gatekeepers to our personal information. ISPs uniquely hold information about many online activities, including information which ties individuals' pseudonymous surfing and downloading activities to their 'real-world' identities. In this context, individuals trust and are dependent on ISPs

[15] *Id.*

[16] *See* Peter Biddle et al., *The Darknet and the Future of Content Distribution, in* Proc. ACM Workshop on Digital Rights Management (2002), *available at* http://crypto.stanford.edu/DRM2002/darknet5.doc; Ian Clarke, *The Philosophy Behind Freenet*, *at* http://freenetproject.org/index.php?page=philosophy&PHPSESSID=fca0b9ec8c97a47974 56a0c20a26097a; George F. du Pont, *The Time has Come for Limited Liability for Operators of True Anonymity Remailers in Cyberspace: An Examination of the Possibilities and Perils*, 6-Fall J. Tech. L. & Pol'y 3 (2001); Tal Z. Zarsky, *Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet Society*, 58 U. Miami L. Rev. 991 (2004).

to safeguard sensitive personal information and communications. Indeed, given the relationship between some ISPs and their subscribers, it is possible that the conditions for the imposition of fiduciary duties on ISPs might exist in some cases.[17] Canadian courts, including the Supreme Court of Canada, continue to recognize the importance of maintaining a degree of privacy or confidentiality with respect to the personal information held by ISPs. Especially so when it comes to linking legal names or other common identifiers to particular IP addresses. As one member of the Supreme Court of Canada recently held:

> [an individual's surfing and downloading activities] tend to reveal core biographical information about a person. Privacy interests of individuals will be directly implicated where owners of copyrighted works or their collective societies attempt to retrieve data from Internet Service Providers about an end user's downloading of copyrighted works. We should therefore be chary of adopting a test that may encourage such monitoring.[18]

In *BMG v. Doe*, the Federal Court of Canada was forced to confront the conflict between copyright enforcement and privacy, head-on, when CRIA commenced a litigation campaign against P2P file-sharers 'in parallel' with the one commenced by the Recording Industry Association of America (RIAA). As *BMG v. Doe* ascends through the appellate process, it promises to be an important comparative IP and cyberlaw case, forcing the courts to craft a judicial test for determining when ISPs should be compelled to disclose their customers' identities to copyright owners.

2. *BMG v. DOE*

On March 31, 2004, the Federal Court of Canada issued a widely-publicized ruling in *BMG v. Doe*. This decision propelled Canada into the international spotlight because of the Court's statements regarding the legality of sharing music files on P2P networks.[19] The media coverage

[17] Ian Kerr, *Personal Relationships in the Year 2000: Me and My ISP*, *in* Personal Relationships of Dependence and Interdependence in Law (Law Commission of Canada ed., 2002) 78, 110-11; Ian Kerr, *The Legal Relationship Between Online Service Providers and Users*, 35 Can. Bus. L.J. 40 (2001) [hereinafter Kerr, *Legal Relationship*].

[18] Society of Composers, Authors and Music Publishers of Canada v. Canadian Association of Internet Providers, 2004 SCC 45, at para. 155 (LeBel, J., dissenting) [hereinafter *SOCAN v. CAIP*]. *See also* Irwin Toy Ltd. v. Doe 2000 O.J. No. 3318 (QL) (Ont. S.C.J.) at paras. 10-11.

[19] *See, e.g*, Electronic Privacy Information Center, *Canadian Court OKs peer to peer sharing*, EPIC Alert, Apr. 8, 2004 *at* http://www.epic.org/alert/EPIC_Alert_11.07.html;

tended to obfuscate the other issue central to the decision, which focused on whether the privacy concerns in the case outweighed the interest of a private party in obtaining discovery in civil litigation. *BMG v. Doe* is significant because it may have set the threshold test for future cases in Canada and perhaps elsewhere, where courts are asked to compel ISPs to link individuals' online nyms – specifically their IP addresses – to their offline identities.

2.1 Nature of the case

BMG v. Doe involved an impressive matrix of fifty-three organizations and individuals, divided into four categories as follows:

> *Plaintiffs*: seventeen music recording companies who were members of CRIA (collectively "CRIA");
>
> *Defendants*: twenty-nine unnamed individuals identified only by their P2P pseudonyms and IP addresses;
>
> *Non-party respondents*: five of Canada's largest telecommunications and cable ISPs: Shaw Communications Inc., Telus Inc., Rogers Cable Communications Inc., Bell Sympatico, Vidéotron Ltée. (collectively the "ISPs"); and
>
> *Interveners*: Canadian Internet Policy and Public Interest Clinic (CIPPIC) and Electronic Frontier Canada (collectively the "Interveners").[20]

The case began in February 2004 when CRIA commenced a copyright infringement lawsuit against the Defendants, alleging that the Defendants had unlawfully shared copyrighted music files on P2P networks. CRIA could only identify the Defendants by their P2P pseudonyms and IP addresses.

CRIA immediately brought a preliminary motion (the "Motion") seeking to compel the ISPs to release the identities of the twenty-nine unknown subscribers. The initial reactions of the ISPs differed widely, with Shaw

---

John Borland, *Judge: File Sharing Legal in Canada*, Cnet News.com, Mar. 31, 2004, *at* http://news.com.com/2102-1027_3-5182641.html?tag=st.util.print; *Keep on Swapping! Cdn File Sharers Told*, p2pnet.net News, Mar. 31, 2004, *at* http://p2pnet.net/story/1118; Tony Smith, *File Sharers Not Guilty of Copyright Infringement – Canadian Judge*, The Register, Mar. 31, 2004, *at* http://www.theregister.co.uk/2004/03/31/file_sharers_not_guilty/; Gene J. Koprowski, *Canada Feds Rule Song Swapping Legal*, TechNewsWorld, Apr. 1, 2004, *at* http://www.technewsworld.com/story/33290.html.

[20] It should be noted that co-author of this chapter, Alex Cameron, was also co-counsel for CIPPIC (http://www.cippic.ca) in *BMG v. Doe*.

taking the strongest stand to protect its subscribers' privacy. With the exception of Vidéotron, all of the ISPs opposed the Motion in Federal Court. The Interveners also opposed the Motion.

2.2 Evidence

2.2.1 CRIA's evidence

The bulk of CRIA's evidence in support of the Motion came from Mr. Millin, the President of a company called MediaSentry. MediaSentry is a New York company that CRIA had hired to gather evidence of copyright infringement on P2P networks.

Millin explained that his company had searched P2P networks for files corresponding to CRIA's copyrighted sound recordings and then randomly downloaded such files from each Defendant between October and December 2003. He claimed that MediaSentry was able to determine the IP address of each Defendant at the time MediaSentry downloaded the files. Using the American Registry for Internet Numbers,[21] MediaSentry was then able to determine which ISPs the IP addresses had been assigned to at the relevant times. This allowed MediaSentry to determine the ISP through which each Defendant had been sharing the files.

During cross-examination, Millin admitted that he had not listened to the files that MediaSentry downloaded. He also acknowledged that linking an IP address to a subscriber account would identify only the ISP subscriber, not necessarily the P2P user engaged in file-sharing. For example, Millin admitted that an ISP account may have hundreds of users on a local area network or that a wireless router might be used by any number of authorized and unauthorized users to engage in file-sharing.

Finally, Millin explained that MediaSentry used files called "MediaDecoys" as part of its work with CRIA. These are files that appear to be copyright songs based on their filenames. However, once a P2P user downloads and opens the file, they discover that the file is actually inoperative. Such measures are designed to reduce the attractiveness of P2P networks by frustrating P2P users. Because Millin did not listen to any of the files downloaded by MediaSentry, he admitted that he did not know whether any of those files were in fact MediaDecoy files, thus rendering impossible a determination in any given instance whether CRIA-owned content was in fact being shared.

[21] This is a non-profit organization that assigns IP addresses to ISPs. See http://www.arin.net for a description of this organization.

2.2.2 ISPs' evidence

Three ISPs – Shaw, Telus and Rogers – were the only parties to file evidence opposing the Motion. Neither Bell nor Vidéotron filed evidence and, by order of the Court, the Interveners were not permitted to file evidence.

Shaw and Telus gave evidence that they almost always assigned IP addresses to their subscribers "dynamically." This means that each time a subscriber went online, the subscriber would be randomly assigned a new IP address for that session. Shaw stated that it did not keep historical records of which IP addresses were assigned to particular subscribers at particular times. For this and other technical reasons, Shaw's evidence indicated that it could not, with the degree of certainly required, provide the personal information sought by CRIA. This was a point of difference between the ISPs which is important to bear in mind for the discussion of *Lawful Access* under Part 3 below. Shaw also registered its concern about potential legal liability in fulfilling CRIA's request; for example, the liability that might arise if it incorrectly matched an IP address to a subscriber, even through no fault of its own.

Telus gave evidence that it did not have any records of the information sought by CRIA and that it had no commercial reason to maintain those kinds of records. Multiple databases would have to be cross-referenced in order to search for and produce the information sought by CRIA. Further, Telus stated that the longer the delay between the event and Telus' search, the less reliable the information would become. This turned out to be an important evidentiary point since MediaSentry had gathered CRIA's evidence as early as October 2003, roughly six months before the court hearing. Finally, Telus provided evidence about how responding to CRIA requests would be costly and disruptive to Telus' operations, particularly if such requests were made in significant numbers in the future.

Rogers provided evidence indicating that it had some information about eight of the nine Rogers subscribers targeted by CRIA and that it had sent notice of the CRIA lawsuit to almost all of those subscribers. Rogers indicated that it generally retained the kind of information sought by CRIA for a period of six days.

Although Bell did not file evidence, Bell's counsel advised the Court that Bell had already identified and was holding information about all of the targeted Bell customers. Bell's counsel also echoed concerns raised by the other ISPs about compensation for ISPs' costs to comply with a disclosure order.

2.3 Privacy arguments in *BMG v. Doe*[22]

2.3.1 CRIA's arguments

CRIA argued that the following seven-part test should be applied by the Court in deciding whether to compel disclosure of the identities of the ISP subscribers:

1. Is there a *prima facie*, or *bona fide* case, at least, of copyright infringement?
2. Is there a relationship between the ISPs and the alleged infringers?
3. Do the ISPs have information about the identities of the alleged infringers?
4. Are the ISPs the only practical source of the information sought?
5. Is the information necessary for CRIA to proceed with its lawsuit?
6. Would the information sought be compellable at trial and useful to CRIA's case?
7. Is there any interest, privacy or otherwise, that would outweigh the ISP's duty to disclose the identity of the alleged infringers?

Privacy concerns figure into the first and last elements of this test. They arise under the first element in the sense that privacy concerns might justify a higher evidentiary threshold at the preliminary stage of the lawsuit. For example, the requirement of proving a *prima facie* case of infringement would be a higher threshold than proving a mere *bona fide* (good faith) case. CRIA did not draw a distinction between these evidentiary thresholds, arguing, in any event, that it had satisfied either threshold.

Privacy might arise under the last element of the test as a factor which could prevent disclosure outright. With respect to this element, CRIA argued that there were no privacy concerns at issue in the Motion that would outweigh CRIA's interest in having disclosure in order to sue the alleged infringers.

CRIA asserted that Canadian privacy law did not prevent disclosure because the law expressly permitted disclosure without an individuals' consent where required by an order of a court.[23] CRIA also argued that the ISP subscribers had already consented to disclosure in the circumstances (where violation of a legal right was at issue) by agreeing to such provisions

[22] The written arguments in the case can be accessed online at http://www.cippic.ca/file-sharing-lawsuit-docs. A blog of the oral arguments is also available at http://www.cippic.ca/file-sharing-lawsuits.

[23] Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, ss. 7(3)(c).

in their ISPs "acceptable use" agreements, upon subscribing to the ISPs' services.

CRIA further argued that many of the privacy concerns raised by the other parties to the Motion were diminished by virtue of the fact that there was little likelihood that the Defendants' Internet activities at large would be associated with their actual identities on the basis of merely providing CRIA with the link between their P2P usernames, IP addresses and their legal names, as sought by the order. Finally, in response to the ISP's evidence and arguments, CRIA claimed that the ISPs were able to identify the subscribers because, for example, Shaw and Rogers admitted that they had done so in response to police or other requests on numerous occasions in the past.

2.3.2 ISPs' arguments

Shaw sought to protect its customers' personal information in accordance with Canadian privacy law, in part because it could be held accountable to its customers or to Canada's Federal Privacy Commissioner. Shaw expressly adopted parts of CIPPIC's argument and asserted that there were substantial privacy interests at stake which required the Court to impose a high standard – a "strong *prima facie* case" – on CRIA before ordering disclosure. Shaw argued that the CRIA request amounted to a civil search warrant in circumstances where there was no legal authority for such a warrant and where there were no privacy protections for the targets of the inquiry.

In terms of whether the test had been met, Shaw claimed that CRIA had not made out a *prima facie* case of copyright infringement. For example, Shaw asserted that there was no evidence as to how CRIA linked the P2P pseudonyms to the IP addresses and no evidence that anyone at CRIA had listened to the downloaded songs.

Telus stated that it had no documents sought by CRIA and characterized the Motion as a mandatory order conscripting Telus to conduct investigations for CRIA and to create documents for CRIA without concern for the impact it would have on Telus and without concern for the reliability of the information produced. This was a time-consuming and costly process which would be disruptive to Telus' ordinary course of business. It was also something for which Telus argued it might face liability to its customers. Telus suggested that CRIA should have asked KaZaA and other P2P companies for the information sought before coming to the ISPs.

Rogers made brief arguments, asserting that the order sought by CRIA was extraordinary and that CRIA should be required to produce evidence commensurate with the nature of the order sought. Rogers also asserted that the form of order sought by CRIA should be more restrictive. For example, Rogers submitted that if the order were granted Rogers should only be

required to produce the last known name and address of the account holders at issue.

Finally, Bell took a relatively neutral approach in its argument by highlighting issues and questions that the Court should consider. Bell submitted that the Court should only make an order for disclosure of personal information where the moving party has made out a *prima facie* case based on admissible evidence. Bell asserted that there was no evidence as to how the IP addresses of the alleged Defendants were linked to the pseudonyms and that the affidavits filed by CRIA were not based on personal knowledge.

2.3.3 CIPPIC's arguments

CIPPIC filed a substantial written brief regarding privacy and copyright issues. Drawing on a number of Supreme Court of Canada search and seizure cases and Canada's recently enacted private-sector privacy laws, CIPPIC asserted that there were fundamental privacy values at stake in the case, demanding that a high threshold test be applied before identity should be disclosed. These privacy values included protection of informational privacy which the Supreme Court had expressly recognized in Canada.[24] In explaining why the threshold test was critical from a privacy perspective, CIPPIC pointed to the Supreme Court of Canada decision in *R. v. Dyment* where the court stated that "if privacy of the individual is to be protected, we cannot afford to wait to vindicate it only after it has been violated."[25]

Further justifying a high threshold test, CIPPIC advanced arguments regarding the particular importance of online privacy and anonymity:

> The Internet provides an unprecedented forum for freedom of expression and democracy. The ability to engage in anonymous communications adds significantly to the Internet's value as a forum for free expression. Anonymity permits speakers to communicate unpopular or unconventional ideas without fear of retaliation, harassment, or discrimination. It allows people to explore unconventional ideas and to pursue research on sensitive personal topics without fear of embarrassment.
>
> If the Plaintiffs are able, by virtue of a court order, to link an IP address (*e.g.*, 66.51.0.34) and a KaZaA user name to a presumptive "real world" person, (*e.g.*, John Smith) and thus commence an action against that person, the action could connect information about John Smith to the

[24] R. v. Dyment, 1988 2 S.C.R. 417 at 427-30.
[25] *Id.* at 429-30.

> world (with consequences beyond the scope of the allegation). For example, John Smith might have visited a Web site on sexually-transmitted diseases, posted or shared documents criticizing the government or his employer, discussed his religious beliefs using a pseudonym in a chat room, or virtually any other type of expression. John Smith would likely hold an assumption that he was and would remain anonymous in many of these activities. The effect of the Court order in this case would shatter that anonymity and potentially cause significant embarrassment and irreparable harm to John Smith, independent of and prior to a determination of his culpability. It would have a corresponding chilling effect on free speech and online activity generally.[26]

During oral argument CIPPIC expanded on this hypothetical in response to a question from the Justice von Finckenstein. CIPPIC pointed out that P2P systems can be used to share virtually any kind of document, software, music, video or other file types. In fact CIPPIC was able to point the Court to actual examples of documents and pictures being shared by some of the Defendants. CIPPIC argued that this sharing had been done on an assumption of anonymity and that to reveal the identity of those sharing files would effectively shatter their anonymity much more broadly.

CIPPIC asserted that CRIA should have to provide clear evidence of the alleged infringement, clear evidence of copyright ownership and clear evidence that they have identified the correct defendants. CIPPIC also pointed out that where a case is unlikely to proceed to trial after an interlocutory order is made, courts will and should engage in a more extensive review of the merits of plaintiffs' claims. CIPPIC and Shaw argued that this was important because if disclosure was ordered, CRIA would likely follow the aggressive approach adopted by the RIAA in the US, which pressed defendants to immediately engage in 'settlement discussions' – a potentially problematic practice when one considers the vast inequality in bargaining power between the plaintiff and defendants. CIPPIC argued that a more extensive review of CRIA's case was similarly justified because disclosure of the Defendants' identities could lead to seizure of computers and consequent loss of privacy and the ability to work.

2.4 The decision

The Court began its decision with a cursory review of the facts and then adopted the description of how P2P systems work set forth in *Metro-*

[26] Memorandum of Argument of the Intervener CIPPIC at para. 17-18, BMG v. Doe, 2004 FC 488 (No. T-292-04), *available at* http://www.cippic.ca/en/projects-cases/file-sharing-lawsuits/memorandum_fctd_final_12pt.pdf.

Goldwyn-Mayer Studios Inc. v. Grokster.[27] In terms of the legal issues, the Court framed the case by raising three questions, each of which involves balancing privacy against other considerations: (i) "What legal test should the Court apply before ordering disclosure?"; (ii) "Have the Plaintiffs met the test?"; and (iii) "If an order is issued, what should be the scope and terms of such order?"

2.4.1 What legal test should the Court apply before ordering disclosure?

Following largely on the factors proposed by CRIA, Justice von Finckenstein of the Federal Court held that the following five criteria must be satisfied before a disclosure order would be made:

a) The Plaintiff must establish a *prima facie* case against the Defendants;
b) The ISPs must be in some way involved in the matter under dispute (*i.e.* the ISPs must be more than innocent bystanders);
c) The ISPs must be the only practical source of the information;
d) The ISPs must be reasonably compensated for their expenses arising out of compliance with the order, in addition to their legal costs; and
e) The public interests in favour of disclosure must outweigh legitimate privacy concerns.

These five elements comprise the threshold test established in this case. Although not all of these factors bear on privacy in an obvious way, it is important to consider the Court's findings with respect to each factor because they could have an impact, one characterized as *a broader public interest in privacy*, as discussed below in part 3.

2.4.2 Have the Plaintiffs' met the test?

The Court concluded that CRIA did not meet the test for disclosure because: (i) CRIA did not make out a *prima facie* case, (ii) CRIA did not establish that the ISPs were the only practical source of the information, and (iii) the privacy concerns in the case outweighed the public interest for disclosure. The Court's analysis followed each factor of the threshold test as follows.[28]

Factor 1: CRIA must establish a prima facie case against the Defendants. The Court found that there were three deficiencies in the *prima facie* copyright infringement case advanced by CRIA. First, the Millin affidavit was deficient because it was not based on personal knowledge and gave no

[27] 259 F. Supp 2d 1029 (C.D. Cal. 2003).
[28] The Court offered most of its analysis between paras. 10-42.

reason for his beliefs. The Court also remarked that Millin had not listened to any of the downloaded files and in particular did not know if they were MediaDecoy files. On this basis, it concluded that there was "no evidence before the Court as to whether or not the files offered for uploading are infringed files of the Plaintiffs"[29]

Second, the Court noted that Millin had not explained how MediaSentry linked the P2P pseudonyms to specific IP addresses. Therefore, the Court concluded that it would "irresponsible" for the Court to order disclosure:

> There is no evidence explaining how the pseudonym "Geekboy@KaZaA" was linked to IP address 24.84.179.98 in the first place. Without any evidence at all as to how IP address 24.84.179.98 has been traced to Geekboy@KaZaA, and without being satisfied that such evidence is reliable, it would be irresponsible for the Court to order the disclosure of the name of the account holder of IP address 24.84.179.98 and expose this individual to a law suit by the plaintiffs.[30]

Finally, Justice von Finckenstein found that CRIA had not provided any evidence that copyright infringement had taken place under Canadian law. The Court rejected each of CRIA's infringement claims, noting *inter alia* that "No evidence was presented that the alleged infringers either distributed or authorized the reproduction of sound recordings. They merely placed personal copies into their shared directories which were accessible by other computer user via a P2P service."[31] In part, the Court relied on the landmark Supreme Court of Canada decision in *CCH Canada Ltd. v. Law Society of Upper Canada*,[32] holding that providing facilities to copy does not by itself amount to authorizing infringement. Justice von Finckenstein also held that distribution requires a positive act by the owner of a shared directory, beyond merely placing a file in a shared directory.

Factor 2: The ISPs must be more than innocent bystanders. The Court found that the ISPs were not mere bystanders because they are the means by which file-sharers access the Internet and connect with one another. Although the Court did not specifically say so, its recognition that ISPs play the role of gatekeeper is consistent with view that there is a legal relationship between ISPs and those who use their services, a relationship which may create privacy-related obligations that do not exist for innocent bystanders.

[29] BMG v. Doe, 2004 FC 488 at para. 19.

[30] *Id*. at para. 20.

[31] *Id*. at para. 26.

[32] 2004 SCC 13. *See generally* Michael Geist, *Banner year for digital decisions*, Toronto Star, Dec. 20, 2004 (hailing *CCH Canada Ltd. v. Law Society of Upper Canada* as "the most important copyright case of the year"), *available at* http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_PrintFriendly&c=Article&cid=1103496608921&call_pageid=968350072197.

Factor 3: The ISPs must be the only practical source of the information. The Court found that it could not make a determination on this issue because CRIA had not described the entities that operate P2P systems, where they are located or whether the names corresponding to the pseudonyms could be obtained from the P2P operators. For example, Telus' evidence suggested that CRIA may be able to obtain the identities from KaZaA in cases where users had signed up for 'KaZaA Plus' and would therefore be billed by KaZaA.

Factor 4: The ISPs must be reasonably compensated for their expenses. The Court concluded that the process sought to be imposed by CRIA would be costly and divert the ISPs' resources from other tasks. The Court held that ISPs would need to be compensated for their reasonable costs as well as their legal costs of responding to the Motion.

Factor 5: The public interests in favour of disclosure must outweigh legitimate privacy concerns. The Court began the heart of its privacy analysis by noting that "it is unquestionable but that the protection of privacy is of utmost importance to Canadian society."[33] The Court cited with approval passages from *Irwin Toy v. Doe*, which articulated the value of privacy on the Internet:

> 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.[34]

The Court in *BMG v. Doe* noted, however, that privacy is not absolute and cannot be used to insulate anonymous persons from civil or criminal liability. Because courts are required to balance privacy rights against the rights of other individuals and in light of the public interest, the Court recognized that CRIA had legitimate copyrights in their works and were entitled to protect them against infringement. Thus, the Court recognized that CRIA had an interest in compelling disclosure of the identities of the peer-to-peer file-sharers. The Court also implied that there was a public interest favouring disclosure in litigation so that parties are not denied the ability to bring and try their legal claims merely because they cannot identify

[33] BMG v. Doe, 2004 FC 488 at para. 36.

[34] *Id.* at para. 37 (quoting Irwin Toy Ltd. v. Doe (2000), 12 C.P.C. (5th) 103 (Ont. Sup. Ct.) at paras. 10-11).

the alleged wrongdoers.[35] Consequently, it held that the privacy concerns in the case must be balanced against CRIA's interest and the broader interest that it stands for.

In its analysis of the privacy concerns, the Court held that the reliability and scope of the personal information sought by CRIA were the most significant factors to consider. The information sought must be reliable and ought not to exceed the minimum that would be necessary in order to permit CRIA to identify the alleged wrongdoers.[36] Here, the Court held that CRIA had sought too much information from the ISPs and that the information sought was not sufficiently reliable to justify disclosure:

> 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 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*.[37]

In the above passage, the Court expressly mentions the age of the data as contributing to its unreliability. Perhaps even more importantly, its reference to the "serious possibility of an innocent account holder being identified" ought to be understood in reference to the lack of an evidentiary link between the P2P pseudonyms and IP addresses. Even on the assumption that a given ISP is able to accurately link IP addresses to its customers' legal names, without being able to prove the connection between online pseudonyms and IP addresses, the Court determined that CRIA is unable to ensure that it is seeking to compel disclosure of the identities of the appropriate individuals. As a result of these weighty privacy concerns, the Court refused to compel disclosure.

2.4.3 If an order is issued, what should be the scope and terms of such order?

Although the Court did not order disclosure in this case, it did propose a privacy-protective framework for orders that might be granted in future cases. The Court noted that if an order for disclosure had been made, certain

[35] *Id*. at para. 42.
[36] *Id*.
[37] *Id*. (emphasis added).

restrictions would have been needed to protect the privacy of the Defendants because "the invasion of privacy should always be as limited as possible."[38]

First, the use of subscriber names by CRIA would be strictly limited to substituting the John Doe and Jane Doe names in the lawsuit. Second, only the P2P pseudonyms would be used as a proxy for the legal names for the Defendants on the Statement of Claim. This would protect the names of the subscribers from public disclosure, at least initially. An annex (protected by a confidentiality order) would be added to the Statement of Claim relating each P2P pseudonym to the legal name and address of a particular ISP account holder. Finally, the ISPs would only be required to disclose the name and last known address of the account holders. These kinds of protections would provide the information CRIA needed to proceed with a given claim while, at the same time, providing a measure of privacy protection to Defendants.

3. LESSONS FROM *BMG v. DOE*

The decision in *BMG v. Doe* has precipitated two significant events in Canada. First, CRIA commenced an appeal of the decision to Canada's Federal Court of Appeal. That appeal is set to be heard on April 20-21, 2005. Second, CRIA has continued its lobbying efforts to persuade the Government of Canada to ratify the *WIPO Copyright Treaty* and *WIPO Performances and Phonograms Treaty*.[39] Though implementation of the treaties has not yet happened, some think it imminent.[40] These copyright

[38] *Id*. at para. 44.

[39] World Intellectual Property Organisation Copyright Treaty, Dec. 20, 1996, S. Treaty Doc. No.105-17 at 1 (1997), 36 I.L.M. 65; World Intellectual Property Organisation Performances and Phonograms Treaty, Dec. 20, 1996, S. Treaty Doc. No.105-17 at 18 (1997), 36 I.L.M. 76 (providing "adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors [performers or producers of phonogram] in connection with the exercise of their rights under [those] Treaties"). Interestingly, the lobbying has proceeded in both directions. In addition to CRIA lobbying the Canadian government, Canadian politicians made public promises to the recording industry – just prior to Canada's most recent Federal election – that the Government would respond to the decision through legislation. *See, e.g.*, *Scherrer vows to crack down on file sharers*, CBC News Online, Apr. 13, 2004, *at* http://www.cbc.ca/arts/stories/scherrer20040413; Press Release, CRIA, The Canadian recording industry calls for adoption of Heritage Committee copyright report recommendations (May 12, 2004), *available at* http://www.cria.ca/news/120504a_n.php.

[40] *See, e.g.*, Michael Geist, *'TPMs': A Perfect Storm For Consumers*, The Toronto Star, Jan. 31, 2005, *available at* http://geistcanadiandmca.notlong.com; Ian Kerr, Alana Maurushat, & Christian S. Tacit, *Technical Protection Measures: Part II – The Legal Protection of*

wars, pitting our cultural industries against various segments of the general population, have received much attention. However, the possible ramifications of these battles for online privacy have received considerably less airplay.

On one hand, *BMG v. Doe* sends a clear message to future plaintiffs – they should come to court with solid evidence of the alleged wrongdoing as well as solid evidence of a reliable link between the alleged activity and specific individuals. Without this kind of evidence, privacy concerns may militate against disclosure, as they did in this case. Further, even where privacy concerns do not justify refusing disclosure outright, the Court also sent a message to future courts that any invasion of privacy should be limited and minimized by protective measures in the disclosure order. For these reasons, *BMG v. Doe* must unquestionably be read as a victory for privacy and as an endorsement for preserving online anonymity unless there are strong reasons to justify compelling the disclosure of identity.

On the other hand, however, a number of the Court's findings in *BMG v. Doe* may quite unintentionally diminish Internet privacy in the future. Recall that the result in *BMG v. Doe* turned on the inadequate evidence provided by CRIA. The decision openly invites CRIA to come back to court with better evidence of wrongdoing in a future case. Such an invitation may well result in even closer scrutiny of Internet users targeted by CRIA, both to establish a reliable link between their pseudonyms and their IP address and to carefully document the kinds of activities that the individuals were engaged in for the purpose of attempting to show a *prima facie* copyright violation.[41] It could also motivate the development of even more powerful, more invasive, surreptitious technological means of tracking people online. This increased surveillance might be seen as necessary by potential litigants in any number of situations where one party to an action, seeking to compel disclosure of identity information from an ISP, is motivated to spy on the other, set traps and perhaps even create new nyms in order to impersonate other peer-to-peer file-sharers with the hope of frustrating them, intimidating them, or building a strong *prima facie* case against them.

Still, there are good reasons in favour of upholding the decision in *BMG v. Doe* on appeal. Independent of the copyright claims, the serious deficiencies in CRIA's evidence – particularly the lack of a link between the

---

TPMs (2002), *available at* http://www.pch.gc.ca/progs/ac-ca/progs/pda-cpb/pubs/protectionII/index_e.cfm.

[41] While monitoring the activities of peer-to-peer file sharers may achieve these objectives, surveillance can also be used as a broader means of social manipulation or control. *See, e.g.*, James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. Cin. L. Rev. 177 (1997); Oscar H. Gandy, Jr., The Panoptic Sort: A Political Economy of Personal Information (1993); Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination (David Lyon ed., 2002).

pseudonyms and the IP addresses – is itself a sufficient reason to reject disclosure, even if privacy protections were built into an order. In its appeal factum, CIPPIC elaborates on the reasons why the evidentiary issues are so important:

> The Appellants [CRIA] have relied upon automated computer systems to gather and generate evidence in support of their motion. They have not disclosed the details of how these systems work. Without explaining how the error was made, the Appellants admit that they made an error in one of the IP addresses at issue - rather than 64.231.255.184, one of the targeted IP addresses should be 64.231.254.117.
>
> …
>
> When dealing with this kind of evidence in support of such extraordinary *ex parte* relief, the court should be presented with frank and full disclosure. For example, full disclosure might include an explanation from an independent expert as to how the P2P pseudonyms are linked to IP addresses (along with a solid documentary backup to put the explanation beyond doubt in every case). One incorrect number in an IP address means all the difference to the innocent person that would exposed by the order sought.[42]

The real challenge for the Federal Court of Appeal in the *BMG v. Doe* case will not simply be the determination of whether or not to grant a disclosure order. The real challenge will be to formulate and then clearly articulate general principles about how to account for privacy and other interests in a way that accommodates the many concerns expressed above. In so doing, it will be crucial for the Court to recognize that any such exercise does not merely involve weighing the privacy interests of the individual defendants against CRIA and the public interest in permitting parties to proceed with lawsuits. *There is a broader public interest in privacy that must also be considered.*

This broader public interest in privacy on the Internet has been hinted at in other Canadian cases.[43] To the extent that the Court's order in *BMG v.*

[42] Memorandum of Fact and Law of the Intervener CIPPIC at paras. 7 and 36, BMG Canada Inc. v. John Doe, 2004 FC 488, *appeal filed*, No. A-T-292-04 (F.C.A. Apr. 13, 2004), *available at* http://www.cippic.ca/en/projects-cases/file-sharing-lawsuits/CIPPIC%20FINAL%20Factum%20Aug%2010%202004.pdf

[43] *See, e.g.*, Irwin Toy Ltd. v. Doe 2000 O.J. No. 3318 (QL) (Ont. S.C.J.) at para. 10 ("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"); *SOCAN v. CAIP*, *supra* note 18, at para. 155

Doe may result in privacy invasions through increased monitoring and surreptitious surveillance, this broader-based public interest in privacy must be taken into account in the analysis of how, when and why disclosure should be ordered or rejected. As one Supreme Court of Canada Justice recently acknowledged, courts considering the intersection of copyright and privacy should "be chary of adopting a test that may encourage [the monitoring of an individual's surfing and downloading activities]."[44]

One final lesson to be learned from *BMG v. Doe* is that the view of the ISP as the trusted guardian of its customers' privacy may soon be relegated to the past.[45] In the early days of the world wide web, most commercial ISPs put a sincere premium on their customers' privacy and, at that time, were in a plausible position to do so.[46] More recently, ISPs have faced a reputational pressure to protect privacy. This pressure is particularly present where one major ISP breaks from the pack and indicates that it will protect its subscribers' privacy, thereby creating intense pressure for other ISPs to follow suit.

However, in the time that has passed since those heady days, the ISP-customer relationship has become more complex.[47] Although some of the ISPs involved in *BMG v. Doe* continue to play a role in advocating their customers' privacy, perhaps partly as a result of the pressure imposed by Shaw's strong lead to protect privacy in the case, others have chosen to play a lesser role, despite indications in their corporate privacy policies that claim a "longstanding commitment to safeguarding [subscribers'] right to

---

("Privacy interests of individuals will be directly implicated where owners of copyrighted works or their collective societies attempt to retrieve data from Internet Service Providers about an end user's downloading of copyrighted works") (LeBel, J., dissenting).

[44] *SOCAN v. CAIP*, *supra* note 18, at para. 155 (LeBel, J., dissenting). Although Justice LeBel was discussing a test for jurisdiction, his rationale in that context seems to apply even more so to the issue of the *BMG v. Doe* threshold for compelling the disclosure of identity.

[45] For a better understanding of those heady days, see generally Kerr, *Legal Relationship*, *supra* note 17.

[46] From time to time one still hears this. *See, e.g.*, Declan McCullagh, *Verizon appeals RIAA subpoena win*, Cnet News.com, Jan. 30, 2003 (in the context of the RIAA lawsuits in the United States, Verizon stated that it would "use every legal means to protect its subscribers' privacy"), *at* http://news.com.com/2100-1023-982809.html. One may wonder whether such litigation is motivated more by user privacy or the administrative cost to ISPs in complying with disclosure demands.

[47] *See generally* Alex Cameron, Pipefitting for Privacy: Internet service providers, privacy and DRM, Presentation to the 5th Annual Center for Intellectual Property Law and Information Technology Symposium at dePaul University College of Law: Privacy and Identity: The Promise and Perils of a Technological Age (Oct. 14, 2004).

privacy"[48] and an "eager[ness] to ensure protection of information carried over the Internet and respect for [subscribers'] privacy."[49]

One reason for this may be that the business of ISPs is no longer merely that of providing Internet access. For example, some Canadian ISPs have entered into the music downloading business.[50] Bell offers its customers music downloading through a service called Puretracks.[51] Vidéotron, on the other hand, is wholly owned by Quebecor Media Inc.[52] which provides its own music downloading service through another subsidiary company, Archambault Group Inc.[53] It should come as no surprise, therefore, that Vidéotron did not oppose CRIA's motion in *BMG v. Doe*. In fact, on appeal, Vidéotron has actually *supported* CRIA's position on the copyright issues, leaving little doubt about where it stands on the issues in the case: "[Vidéotron] agrees to protect its clients' privacy. [Vidéotron] does not agree to protect its clients' piracy."[54] As the ISP industry continues to evolve, it will be interesting to see whether other ISPs might follow Vidéotron's example.

Another reason why ISPs are no longer the trusted guardians of privacy they once were is the increasing role that ISPs are being forced to play in aiding international law enforcement and the fight against cybercrime and terrorism.[55] Recognizing that ISPs are not only the pipeline of online communication but also the reservoirs of their customers' personal information and private communications, cybercrime legislation proposed or enacted in many jurisdictions – including legislative reforms currently under

[48] Bell, Customer Privacy Policy, *at* http://www.bell.ca/shop/en/jsp/content/cust_care/docs/bccpp.pdf.

[49] Vidéotron, Legal Notes, *at* http://www.videotron.com/services/en/legal/0_4.jsp.

[50] *See, e.g.*, Press Release, BCE, Bell Canada Launches the Sympatico Music Store (May 13, 2004), *available at* http://www.bce.ca/en/news/releases/bc/2004/05/13/71214.html.

[51] *Id*. Another Canadian ISP, Telus, is also offering music downloads in conjunction with Puretracks which can be accessed at http://telus.puretracks.com/. In addition to possibly helping to attract and retain customers, such services provide ISPs with an alternative revenue stream outside of charging a flat fee for access to the Internet.

[52] For a description of Vidéotron's relationship with Quebecor Media Inc., see http://www.videotron.com/services/en/videotron/9.jsp.

[53] See http://www.archambault.ca for a description of this company and its services.

[54] Memorandum of Fact and Law of the Third Party Respondent Vidéotron Ltée at para.7, BMG v. Doe, 2004 FC 488, *appeal filed*, No. A-T-292-04 (F.C.A. Apr. 13, 2004), *at* http://www.cippic.ca/en/projects-cases/file-sharing-lawsuits/videotron_factum.pdf.

[55] *See, e.g.*, Convention on Cybercrime, Nov. 23, 2001, Europ. T.S. No. 185, *available at* http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG. *See also* Ian R. Kerr & Daphne Gilbert, *The Changing Role of ISPs in the Investigation of Cybercrime*, *in* Information Ethics in an Electronic Age: Current Issues in Africa and the World (Thomas Mendina & Johannes Brtiz eds., 2004).

consideration in Canada[56] – will be used to expedite criminal investigations by substantially reducing the threshold tests required to obtain a judicial order for various forms of state surveillance. In other words, ISPs will be compelled to disclose identity information in a number of circumstances without anyone having to come before a judge and prove that the privacy rights of the individual under investigation and the broader public interest in protecting personal privacy are outweighed by the public interest in investigating cybercrime.

Canada's *Lawful Access*[57] agenda is one example of where ISPs may be forced to play a bigger role in aiding law enforcement. Under the current system, each major ISP in Canada has a different network architecture. The differences can be particularly significant between telecommunications and cable ISPs. These differences have important implications for privacy protection because the ability of each ISP to capture and retain information relating to the identity of their subscribers can differ greatly. This difference is reflected in the different ISP responses in the *BMG v. Doe* case – for example, Shaw and Telus claimed that they had none of the information sought by CRIA and Bell claimed that it had all of the information. Under *Lawful Access*, this will change as certain providers will be forced to completely re-engineer their networks to provide law enforcement with easy access to data.

As Professor Michael Geist has noted, *Lawful Access* will create a baseline standard for all ISPs data retention and network configurations that will make it far easier for identity information to be obtained from them. This easier access to identity information will undoubtedly spill over from the law enforcement context to the civil actions. At the very least, ISPs will no longer be able to argue that they do not have the information sought. The reputational pressure on ISPs to protect privacy may also become negligible.

Finally, cost is another reason why ISPs may no longer be trusted guardians of privacy. When law enforcement or private parties have knocked on ISPs' doors seeking identity information to date, the first concern of the ISPs has often been "Who is going to pay for this?". Provided that ISPs are reimbursed for their costs of providing the information, ISPs will likely put up little privacy-based resistance to initiatives like *Lawful Access* and notice-

[56] Dept. of Justice et al., *Lawful Access: Consultation Document* (Aug. 25, 2002), *available at* http://canada.justice.gc.ca/en/cons/la_al/law_access.pdf.

[57] "Lawful Access" is the euphemism designated to describe the Government of Canada's attempt to modernize law enforcement by expediting various forms of investigatory procedures, including procedures by which law enforcement agencies are able to more easily obtain identity information and personal communications from ISPs (in some cases without going to court). The Department of Justice is currently in the midst of an extensive "Lawful Access Consultation" process. For a description of this process and documents related to it, see http://canada.justice.gc.ca/en/cons/la_al/.

and-takedown, or in civil actions like *BMG v. Doe*. Cost was a central issue for the ISPs in *BMG v. Doe*. At times during the hearing, it seemed as though the ISPs and CRIA were effectively engaged in a negotiation, mediated by the court, about how much subscriber's privacy rights could be bought for.

As is the case in private sector disputes such as *BMG v. Doe*, some members of Canadian civil society[58] are also intervening in public sector hearings in order to ensure that the legal thresholds for compelling ISPs to disclose their customer's personal identity information are not diminished in the public law context as a result of Canada's *Lawful Access* agenda.

4. CONCLUSION

As *BMG v. Doe* ascends through the appellate process, it is uncertain whether the *privacy values* articulated by the Federal Court – in a case that will ultimately become known and remembered as *a-case-about-copyright* – will be affirmed and instantiated on appeal. We live in interesting times. At the same time that CRIA and other powerful private sector entities continuously intensify their growing arsenals of powerful new surveillance technologies, governments are seeking to pass laws which make it easier to obtain and make use of the personal information and communications that those private sector surveillance technologies are able to collect in their ever-growing databases, often without the consent of those about whom the information is being collected, used or disclosed to others.

The progression of *BMG v. Doe* through the courts runs 'in parallel' to the development of cybercrime legislation in government. Both of these private and public sector decision-making processes run the risk of diminishing online privacy in favour of an alleged public interest said to conflict with it.

One of the pioneers of the Internet, Stewart Brand, famously said that: "[o]nce a new technology rolls over you, if you're not part of the steamroller, you're part of the road."[59] This unseemly prospect is so powerful, so compelling that it paves an attitude in some of those in opposition to the value set underlying the dominant technology to develop bigger steamrollers and steer them in the opposite direction. There is little doubt that for a small subset of those who cherish P2P file-sharing, the answer to CRIA and surveillance technologies like those used by

[58] Canadian civil society groups include: On the Identity Trail (http://www.anonequity.org), CIPPIC (http://www.cippic.ca), Public Interest Advocacy Center (http://www.piac.org), and the B.C. Civil Liberties Association (http://www.bccla.org/)..

[59] Stewart Brand, The Media Lab: Inventing the Future at MIT (1987) 9.

MediaSentry will be the development of an extremely potent anonymous P2P network.[60] Such systems would enable Lessig's horrific vision: "[p]erfect anonymity makes perfect crime possible."[61]

For the many netizens who see social value in the ability to exist online and off in various states of nymity, and who abhor those others who intentionally exploit anonymity as nothing more that a means of escaping accountability for immoral or illegal acts, the steamroller mentality is not a promising road. Our courts and legislatures need desperately to pave other paths.

ACKNOWLEDGEMENTS

Ian Kerr wishes to extend his gratitude to the Social Sciences and Humanities Research Council, to the Canada Research Chair program, to Bell, Canada and to the Ontario Research Network in Electronic Commerce for all of their generous contributions to the funding of the research project from which this paper derives: *On the Identity Trail: Understanding the Importance and Impact of Anonymity and Authentication in a Networked Societ*" (www.anonequity.org). Alex Cameron wishes to thank Philippa Lawson for the privilege of representing CIPPIC (www.cippic.ca) in *BMG v. Doe* and Ian Kerr for his steadfast encouragement and support. Both authors are grateful to Todd Mandel for his very capable research support and his outstanding contributions to this project. The authors also wish to express their sincere thanks to Professors Jane Bailey, Michael Geist, and Philippa Lawson for their very helpful comments, which resulted in a much better chapter. Finally, the authors wish to congratulate Katherine Strandburg and Daniela Stan Raicu for organizing CIPLIT's successful 2004 symposium "Privacy and Identity: The Promise and Perils of a Technological Age" at Depaul University College of Law.

[60] Biddle et al., *supra* note 16. *See also* John Borland, *Covering tracks: New privacy hope for P2P*, Cnet News.com, Feb. 24, 2004, *at* http://news.com.com/2100-1027-5164413.html.

[61] Lessig, *supra* note 10, at 1750.