Canadian Journal of Law and Technology

Volume 4 | Number 3 Article 2

8-1-2005

Unmasking the John Does of Cyberspace: Surveillance by Private Copyright Owners

Amy Min-Chee Fong

Unmasking the John Does of Cyberspace: Surveillance by Private Copyright Owners

Amy Min-Chee Fong†

Introduction

As the Internet develops and expands, an increasing number of people are spying on cyberspace activities for various motives, whether commercial, law enforcement, academic research, criminal, or otherwise. In particular, in recent years, private copyright owners have begun to surveil Internet file-sharing activities in order to monitor acts of copyright infringement. After gathering evidence of infringement, some copyright owners have initiated John Doe lawsuits against anonymous alleged wrongdoers and have applied to court for orders requiring Internet Service Providers (ISPs) to reveal the identities of the wrongdoers. Courts are then faced with the task of balancing the Internet user's right to privacy against the copyright owners' intellectual property rights.

Surveillance by private copyright owners is eroding Internet users' rights to privacy. The surveillance is difficult to justify because copyright law is complex and uncertain. In fact, many users do not know whether their activities constitute copyright infringement. Many users are also unaware of the serious consequences of being targeted for copyright infringement. If courts order the disclosure of Internet users' personal information on a low threshold test, then intellectual property rights may be protected at great cost to users' privacy rights.

The goals of this paper are to: (1) explore the expectations of cyberspace privacy in a peer-to-peer context; (2) examine the consequences to Internet users arising from the surveillance tactics of private copyright owners; and (3) discuss possible ways in which a balance can be achieved between privacy and intellectual property rights. Part II of this paper sets out the meaning of information privacy, discusses the widespread use of peer-to-peer networks for trading copyrighted content, and examines the expectations of privacy in peer-to-peer networks. Part III discusses the surveillance tactics of private copyright owners, and explains how the surveillance of alleged wrongdoers is potentially harmful for Internet users. Finally, Part IV examines how ISPs and the judiciary can ensure that an appropriate balance is struck between the privacy rights of Internet users and the interests of copyright owners.

Privacy in Cyberspace

The Meaning of Information Privacy

The meaning of privacy has been the subject of much academic discussion. Edward Bloustein suggests that privacy protects "inviolate personality" and is grounded in respect for individual dignity and personal autonomy.[1] Ruth Gavison suggests that privacy is related to concerns about limiting our accessibility to others.[2] For the purposes of this paper, privacy is defined as the ability to control how personal information is collected, used, and disclosed. This meaning of privacy, referred to as "information privacy",[3] is particularly relevant to cyberspace, where enormous amounts of data are generated, searched, recorded, and exchanged through a continuous stream of transactions conducted by millions of Internet users.

Information privacy protects us from unwanted access by others to our personal information. The *Personal Information Protection and Electronic Documents Act* (PIPEDA),[4] a federal statute governing information privacy in the private sector, defines "personal information" broadly as "information about an identifiable individual".[5] This paper will focus on personal information that is descriptive of an individual's actions and identity in cyberspace.

The right to information privacy must be balanced against other interests, such as the public interest in law enforcement or the rights of other individuals. For the private sector realm, PIPEDA attempts to strike a compromise between the right to information privacy and the need for businesses to collect, use and disclose personal information for "purposes that a reasonable person would consider appropriate in the circumstances".[6] One significant way in which PIPEDA protects information

†B.A.Sc. (University of British Columbia, 2002), LL.B. (University of Victoria, 2005). This paper is the winning entry of the 2005 IT.Can Student Writing Competition.

privacy is by requiring businesses to obtain consent from an individual before collecting, using or disclosing his or her personal information.[7] PIPEDA also lists specific situations where a business does not have to obtain consent,[8] presumably because in those situations privacy is outweighed by other interests.

Privacy in the Peer-to-Peer Context

It is difficult to determine just how much privacy to expect while conducting online affairs because of the elusive nature of the communication, the rapid pace of technological innovation, the blurring of traditional private and public boundaries, and the absence of national and international borders. Expectations of cyberspace privacy are largely shaped by the context and the application.[9] This paper focuses on expectations of privacy in peer-to-peer networks (also known as "P2P" or "file-sharing" networks) in terms of their technical architecture and social norms.

The Peer-to-Peer Revolution

In a peer-to-peer network, each computer acts as both a client and server: as a client, the computer can download files from other computers, and as a server, the computer makes the contents of its hard drives accessible for downloading by other computers.[10] This model allows each connected peer to exchange files with other computers. In a true peer-to-peer network, there is no central server overseeing the network.[11] Such a decentralized framework makes it difficult to regulate users' exchanges of information or to shut down a peer-to-peer network.[12]

In the last few years, peer-to-peer networks have revolutionized the manner in which information is disseminated over the Internet. Any computer can connect to a peer-to-peer network simply by having the appropriate software installed and activated. Users connected to a peer-to-peer network can search the computers of thousands (or even millions) of other users for specific files, and then download those files quickly, freely and anonymously. The unprecedented ease with which content can be distributed by this framework has engendered a multitude of peer-to-peer networks for the exchange of all types of material, ranging from the legitimate and beneficial (*e.g.* Linux freeware operating systems[13]) to the criminal and harmful (*e.g.* child pornography[14]).

In particular, peer-to-peer networks have become notorious for the exchange of copyrighted songs in compressed MPEG-3 format (MP3s). Napster, launched in July 1999, was one of the first peer-to-peer services to become widely used for MP3 downloading. It attracted 10 million users after its first 9 months of operation, and amassed nearly 80 million users after 18 months.[15] Napster's activities were declared illegal by U.S. courts because Napster's control over a centralized file list made Napster contributorily liable for the copyright infringement of its users.[16] Other peer-to-peer networks, including Kazaa, Morpheus, Grokster, and Gnutella, have since surpassed Napster in popularity and have enabled more downloading.[17] Unlike Napster, these peer-to-peer services do not control a centralized file list. In August 2004, the U.S. Court of Appeals for the Ninth Circuit granted summary judgment in favour of Grokster, finding that Grokster was not liable for the acts of copyright infringement of its users because it did not maintain a centralized file list and did not have the right or ability to supervise users' activities.[18] However, this decision was overturned by a unanimous U.S. Supreme Court in June 2005. Justice Souter stated:

> We hold that one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties.[19]

The Court found that there was evidence that Grokster had induced infringement, in that it aimed to supply services to former Napster users, it failed to take steps to diminish the infringing activity, and it intended to attract a high volume of users to generate more advertising revenue. Accordingly, the Court sent the case back to the district court for reconsideration.

Despite the risk of prosecution by copyright owners, peer-to-peer networks continue to be widely used for the trading of copyrighted content. Sonia Katyal suggests three reasons for the file-sharing phenomenon: (1) users think that they are not being watched or that they can escape detection by maintaining anonymity on the network; (2) peer-to-peer networks enforce social norms of sharing and reciprocity that favour exchanges of copyrighted material; and (3) the ethics and legality of downloading copyrighted content over peer-to-peer networks are ambiguous, since the downloading appears more like "non-commercial home copying of copyrighted content" than stealing in real space.[20] The following discussion explores the assumptions underlying the first reason, namely, whether Internet users have an expectation of privacy on peer-to-peer networks.

Expectations of Privacy

In a peer-to-peer context, there are various types of personal information that an Internet user may wish to protect, including: (1) the files on his or her machine that are accessible by others on the network; (2) the data that he or she exchanges with others on the network; and (3) his or her customer identifying information, which is held by the user's ISP[21] if that user is an actual account holder.[22]

The first type of personal information includes only those files that a user elects to share on the network. In theory, a user can control which files are shared, but given the automated process for connecting to a peer-to-peer network and the affirmative action that is often required to block access to certain file directories, many

file-sharers are not aware of what files they are sharing, or worse, they are not even aware that they are connected to a file-sharing network.[23] Thus, a file-sharer may unwittingly be permitting access to sensitive personal information such as financial records, personal photographs, and e-mail. The privacy concerns arising from the sharing of such information are compounded by the architecture of a peer-to-peer network, which enables users to snoop through others' shared hard drives, undetected and with virtually no restraints.

The second type of personal information is composed of "content" and "non-content" information. Content information is the subject of the communication, for example, an MP3 song. Non-content information, also known as "traffic data", is the string of routing and identifying information that is transmitted by a machine as part of every online communication.[24] Traffic data includes the Internet Protocol (IP) addresses[25] of the originating machine and the recipient, the time that the communication was sent and received, the size of the communication, and the path it followed to the ultimate recipient.[26] Content and non-content information contained in an online communication is accessible by the intended recipient(s); in a peer-to-peer network, this may include all users connected to that network. Thus Internet users with at least a basic understanding of the function of peer-to-peer networks have minimal expectation of privacy in content and non-content information, vis-à-vis other users of the network. However, users on peer-to-peer networks typically counteract this apparent lack of privacy by using pseudonyms to log on to networks. This allows users to communicate and exchange files anonymously.

The third type of personal information includes information that the ISP needs to carry on its business of providing Internet access to its customers. This would include an account holder's name, residential or business address, and telephone number, as well as technical information such as the IP address of the account holder's machine.[27] For billing, maintenance, monitoring, and other purposes, the ISP may also generate logs detailing the Internet traffic of their account holders, including lists of their online points of destination.[28] Given these records, ISPs have the ability to unleash vast quantities of information about an individual's online activities. Fortunately for Internet users, most ISPs are conscious of the need to safeguard personal customer information, because they want to build good customer relations, and because, as of January 1, 2004, Canadian ISPs must comply with PIPEDA (or the provincial equivalent).[29] Under PIPEDA, account holders can expect, with some exceptions, that an ISP will not disclose their customer identifying information without their consent.

The first two types of personal information, which can be described collectively as file-sharing data and communications, are vulnerable to monitoring by any interested third party. This characteristic makes them distinct from the third type (customer identifying information), which is only known by the ISP. As long as customer identifying information is not disclosed, a user can maintain an anonymous online presence and thereby protect privacy in respect of his or her file-sharing data and communications, although the user's online activities may be monitored.

U.S. courts are generally reluctant to recognize any expectation of privacy in a peer-to-peer context even if a user connects to a network using a pseudonym. In *In Re Verizon Internet Services, Inc.*, the trial court suggested that "if an individual subscriber opens his computer to permit others, through peer-to-peer file-sharing, to download materials from that computer, it is hard to understand just what privacy expectation he or she has after essentially opening the computer to the world".[30] Similarly, in *Kennedy*, the trial court found that the defendant had no legitimate expectation of privacy in his customer-identifying information because he had activated his file-sharing mechanism on his home computer, thereby allowing anyone to view his files, which included two images of child pornography.[31] The court therefore concluded that the ISP's disclosure of the defendant's customer- identifying information to state law enforcement did not violate the defendant's Fourth Amendment right to be free from unreasonable search and seizure. The court's reasoning ignored an important social norm of peer-to-peer networks: while Internet users may be willing to share their files with the public, they generally do not expect that their identities will be exposed.[32]

Does an anonymous Internet user have a reasonable expectation that his or her online activities will not be linked to his or her real identity? One Canadian case, *Irwin Toy Ltd. v. Doe*,[33] found that there is such an expectation if the user takes steps to secure his online anonymity, and the user's ISP has committed to protecting against disclosure of the user's identity. In *Irwin Toy*, the plaintiffs had commenced an action against an anonymous e-mail user for sending a defamatory message to the plaintiffs' employees. In considering a motion brought by the plaintiffs to require the ISP to identify the user, Wilkins J. for the Ontario Superior Court of Justice stated:

> [10] Implicit in the passage of information through the internet by utilization of an alias or pseudonym is the mutual understanding that, to some degree, the identity of the source will be concealed. Some internet service providers inform the users of their services that they will safeguard their privacy and/or conceal their identity and, apparently, they even go so far as to have their privacy policies reviewed and audited for compliance. . . .
>
> [11] 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. . . .[34]

However, individuals may not use the cloak of privacy to insulate themselves from criminal or civil liability. Disclosure of personal information is appropriate if privacy interests are outweighed by other interests. Wilkins J. granted the motion in *Irwin Toy* because the plaintiffs had established a *prima facie* case for defamation and breach of confidential information.[35]

Costs of Surveillance

For most people, a certain amount of privacy in their daily activities is guaranteed because it is expensive and difficult to spy on everybody. Thus, most library patrons can be assured that a spy hired by a copyright owner will not follow them in the library, observe what books they take off the shelf and what pages they copy in the photocopying room. In cyberspace, however, the constraints on spying are largely eliminated. Automatic systems can be set up to track several Internet users at once, precisely record their every move, and scan their personal hard drives.[36] This scenario is happening right now in the peer-to-peer context, where private copyright owners are asserting and enforcing their rights by surveilling Internet users' activities for copyright infringement, initiating John Doe lawsuits against anonymous Internet users, and seeking court orders to compel ISPs to unmask the anonymous Internet users. The costs of surveillance to Internet users are threatening to upset the balance between the privacy of users and the interests of copyright owners.

Surveillance by Private Copyright Owners

Copyright owners are not pleased that millions of Internet users are routinely downloading copyrighted materials from the Internet.[37] The music recording industry and, more recently, the motion picture industry,[38] have responded by launching an aggressive campaign against what they perceive to be the rampant propagation of piracy on peer-to-peer networks. The recording industry's first targets were the entities that acted as gatekeepers to copyrighted material.[39] Thus, the recording industry sued ISPs and distributors of peer-to-peer networks for contributory infringement of copyright. However, the courts found that ISPs and decentralized peer-to-peer services acting as mere conduits of information were not liable for authorizing the copyright infringement acts of their users.[40] These court actions failed to stop the file swapping, so the recording industry decided to try another tactic: target the individual Internet users themselves.[41]

Since the music and motion picture industries began pursuing individual users, Internet communications have been subject to continuous and minute scrutiny by Internet specialists and investigative agencies hired by private copyright owners to detect and monitor unauthorized distribution of copyrighted material. One commonly used surveillance method of the Canadian and American music recording industries is to employ "web bots" to find alleged wrongdoers and collect evidence of infringing activities.[42] Web bots are software programs that continually crawl from one server to another in cyberspace, compiling lists of sites having particular characteristics. Web bots are launched in peer-to-peer networks to automatically scan user hard drives for titles of unauthorized copyrighted material.[43] When the web bots find what appears to be infringing material, they match the user's IP address to its ISP and send a copyright violation notice to the ISP. The Recording Industry Association of America (RIAA) has used web bots to issue more than one million copyright violation notices to ISPs on behalf of 750 song writers and performers.[44]

Sonia Katyal describes the surveillance methods of copyright owners as "piracy surveillance". Methods of piracy surveillance have the following characteristics: (1) they are performed by private (non-government) entities; (2) they encompass extrajudicial determinations of copyright infringement; and (3) they are extralegal in nature, in that the surveillance takes place entirely outside of ongoing litigation.[45]

Such online surveillance tactics are technologically unbounded and highly intrusive on an individual's right to information privacy.[46] Moreover, since private actors do not trigger the application of the Charter, [47] the investigative agencies hired by copyright owners are not subject to any restraints on unreasonable search and seizure.[48] Such restraints would otherwise be applicable if the state were to investigate the peer-to-peer activities.

Surveillance by copyright owners is costly for Internet users in several respects. First, it can catch many Internet users by surprise, since many users have an expectation of anonymity and the scope of copyright law is far from clear. Second, surveillance can inaccurately identify alleged wrongdoers. Third, surveillance can lead to serious consequences for the individuals whose identities are revealed. Finally, surveillance can have chilling effects on legitimate file-sharing activities. These concerns are examined in light of a recent Canadian decision *BMG Canada v. John Doe*.

Case Study: *BMG Canada v. John Doe*

In *BMG Canada Inc. v. John Doe*,[49] members of the Canadian Recording Industry Association (CRIA) brought an application under the Federal Court Rules[50] to require five ISPs (Shaw, Rogers, Bell, Telus, and Vidéotron) to disclose the names and addresses of 29 of their account holders. The CRIA had commenced John Doe actions for copyright infringement against 29 defendants who had allegedly downloaded over 1,000 copyrighted music recordings over peer-to-peer networks. To investigate the file-sharing activities of the defendants, the CRIA had hired MediaSentry, a company providing online anti-privacy services. MediaSentry was unable to ascertain the identities of the defendants, but could

determine the pseudonyms and IP addresses they had used for downloading music. The CRIA sought to compel the ISPs to release the names of the account holders having those IP addresses at the material times. The ISPs (except Vidéotron) and public interest groups opposed the order.

In *BMG Canada*, the Federal Court was faced with the task of balancing Internet users' privacy concerns against other interests. The Court noted that ISP account holders have an expectation that their identities will be kept private and confidential, based on sections 3 and 5 of PIPEDA and the terms of their service agreements with the ISPs. However, an ISP can disclose personal information without consent pursuant to a court order under paragraph 7(3)(*c*) of PIPEDA.[51]

The issue before the Court was whether it should order the ISPs to reveal the identities of their customers. The Court held the following as the test for compelling a third party to disclose personal information about an unknown alleged wrongdoer:

> (a) the applicant must establish a *prima facie* case against the unknown alleged wrongdoer;
>
> (b) the person from whom discovery is sought must be in some way involved in the matter under dispute, he must be more than an innocent bystander;
>
> (c) the person from whom discovery is sought must be the only practical source of information available to the applicant;
>
> (d) the person from whom discovery is sought must be reasonably compensated for the expenses of complying with the order in addition to his or her legal costs; and
>
> (e) the public interests in favour of disclosure must outweigh the legitimate privacy concerns.[52]

Applying this test, the Court found that the CRIA had not established a *prima facie* case of copyright infringement because the evidence was deficient in many ways. The affidavits contained hearsay, there was no explanation as to how MediaSentry was able to link the defendants' pseudonyms to specific IP addresses, and there was no evidence that the CRIA owned copyright in the files being shared by the defendants.[53] Further, there was no evidence that the defendants had infringed copyright by reproducing songs, distributing or authorizing the reproduction of songs, or knowingly possessing unauthorized copies for the purpose of unlawful distribution.[54] Given the unreliability of the evidence, the public interests in favour of disclosure did not outweigh the privacy interests. Consequently, the Court denied the application for disclosure.

The CRIA appealed this decision. The Federal Court of Appeal upheld the trial court's decision to refuse disclosure of the defendants' identities, because of the weaknesses in evidence connecting the defendants' pseudonyms to IP addresses. However, the Court of Appeal overturned the trial court's characterization of the first element of the disclosure test. The Court of Appeal held it is sufficient if the applicant shows a *bona fide* claim, which means that he or she intends to bring an action for copyright infringement based upon the information obtained, and there is no other improper purpose for seeking the identity of the defendants.[55]

Catching Internet Users by Surprise

The Federal Court's findings on copyright law and file-sharing in *BMG Canada* directly conflicted with the CRIA's allegations of copyright infringement. The Federal Court of Appeal chose not to take sides on this issue. It did not reverse or uphold the trial court's findings on copyright law, but simply stated that such findings were premature and should be reserved for a future case.[56] The indeterminate state of copyright law is one of the problems in this issue: private copyright owners are monitoring peer-to-peer networks under the assumption that users have offended copyright laws. The CRIA was effectively making an extrajudicial determination of the law and catching many Internet users by surprise by their surveillance tactics.

While pervasive, non-obtrusive online surveillance by the state may be justified for investigations of serious threats to public safety or national security,[57] surveillance is not as easily justified when used by private actors to monitor activities that are governed by grey areas of civil law such as copyright law. Particularly as applied to the Internet, copyright law is often complex and murky because it cannot keep pace with the technological developments, and the legislature and courts often fail to give clear directions as to the law.[58] At any given time, millions of Internet users are on peer-to-peer networks swapping copyrighted songs. Many of these users are uncertain as to whether their activities amount to copyright infringement, or whether they have a valid defence under the private use or fair dealing exceptions of the *Copyright Act*.[59] Many users are also not aware that their activities are being tracked by copyright owners intent on pursuing John Doe lawsuits and disclosure applications to unmask the user identities. This lack of awareness is especially true for children. A significant proportion of children are downloading copyrighted material from the Internet,[60] probably because many do not fully understand the legal implications of their activities.

The murkiness of copyright law has led to different characterizations of file-sharing. Supporters of file-sharing put the emphasis on "sharing" and compare the activity to children taping each others' records for private use. The only difference between online file-sharing and taping other children's records is in the magnitude of the sharing: "[w]ith a P2P system, you can share your favorite songs with your best friend — or your 20,000 best friends."[61] On the other hand, the music recording industry takes the view that file-sharing of MP3s is copyright infringement and is comparable to stealing several CDs from a store.[62]

In the United States., the courts have sided with the recording industry and found that the trading of copyrighted content over peer-to-peer networks infringes the copyright owner's exclusive rights to reproduction and distribution.[63] In Canada, the Federal Court in *BMG Canada* went the opposite route by suggesting that a user does not infringe copyright by downloading songs for personal use.[64] The Court based its finding on section 80 of the *Copyright Act*, which provides that it is not an infringement of copyright to reproduce a musical work "onto an audio recording medium for the private use of the person who makes the copy".[65] The *Copyright Act* permits levies to be imposed on blank audio recording media to compensate authors, performers, and makers of sound recordings for copying for private use.[66] Howard Knopf, a lawyer for the Canadian Internet Policy and Public Interest Clinic, explained that the trial judge's finding in *BMG Canada* meant that "[d]ownloading music for personal use is perfectly legal in Canada as the *quid pro quo* for the music industry's legislated levy scheme, which has generated about $100 million to date".[67] However, the Federal Court of Appeal in *BMG Canada* ruled that the Federal Court's findings on copyright law should not have been made at the very preliminary stages of an action, without consideration of all the evidence and applicable legal principles.[68]

Whether or not the Federal Court's interpretation is upheld in a future case, it is important to recognize that not all kinds of file-sharing of copyrighted content are clearly illegal or harmful. For example, Internet users may use file-sharing to download a song that is no longer "in print"[69] and to download a song that is not copyrighted or the copyright owner wants to give away.[70] However, to the surprise of many Internet users, the CRIA in *BMG Canada* determined file-sharing of MP3s to be illegal, actively monitored peer-to-peer networks, and brought court applications to reveal the identities of Internet users. This intrusion on Internet users' expectations of privacy is difficult to justify when the limitations of copyright law are far from certain.

Risks of Mistaken Identification

Not only is the law unclear, but it is unclear who the alleged wrongdoers actually are. In fact, there is a serious possibility that innocent Internet users could become accidentally caught in the electronic net of surveillance. This was recognized by the Federal Court in *BMG Canada*, which held that given the unreliability of the evidence matching IP addresses and pseudonyms to account holders, it would be "irresponsible" to order the disclosure of the identity of an account holder and expose that individual to a law suit.[71]

The facts of *BMG Canada* illustrate the difficulties with identifying alleged wrongdoers in cyberspace. Each ISP is allocated a block of IP addresses from the American Registry for Internet Numbers. The ISP subsequently assigns these IP addresses to its account holders.[72] There are more account holders than there are the number of available IP addresses, but not all account holders are simultaneously connected to the Internet.[73] Most IP addresses are dynamic, which means that a different IP address is temporarily assigned to an account holder's computer each time he or she connects to the Internet.[74] In this way, a given IP address can be reallocated to several users over the course of a day. In order for an ISP to determine the account holder for an IP address at a certain time, the ISP must cross-reference several different databases.[75] The older the information is, the more difficult it is to retrieve, and the more unreliable the result that will be produced.[76] Some ISPs have hundreds of thousands of account holders that are assigned IP addresses as needed in no particular sequence.[77]

Even if an ISP has the necessary data concerning an IP address, at best the ISP can identify the account holder, but not the actual user of the computer.[78] The account holder may not be the individual who is using the computer. For example, the account holder's family member may be the individual behind the online activities.[79] To complicate matters further, it is common for an account holder to set up a Local Area Network (LAN) using a router to share the Internet connection between multiple computers.[80] The ISP can only identify the IP address of the router, not the actual computer that was responsible for a particular online transaction.[81]

Thus, given merely an IP address, it is not necessarily possible to determine who was actually using a computer at a particular time. In the case of a LAN, one of several computers could be the culprit. The inherent problems with identifying Internet users mean that innocent individuals could have their identities exposed by disclosure orders. They would then face costly legal battles to defend against the copyright owners' allegations.

Consequences of Being Unmasked

There are serious consequences facing an Internet account holder should his or her identity be revealed by an ISP to a copyright owner. The account holder may face *ex parte* orders to have his or her computer seized to preserve and analyze evidence.[82] Large amounts of personal information on the hard drives could be searched. An account holder who lacks the resources to defend against an expensive lawsuit may be forced into settling with the copyright owner.[83]

Moreover, if the account holder does not settle and is then found liable for copyright infringement at trial, he or she may have to pay substantial damages. An individual who downloads MP3 songs may be sued for copyright infringement by a copyright owner who may demand statutory damages per work of $500 to $20,000.[84] If the identities of the defendants in *BMG Canada* were to be revealed, the CRIA could seek at least

$500,000 in statutory damages per defendant, based on the CRIA's estimate that each defendant had downloaded more than 1,000 songs over which the CRIA had copyright.[85] It is unlikely that the defendants were aware that their file-sharing activities would attract the risk of such a severe penalty. The foregoing consequences exacerbate the privacy concerns of unmasking anonymous Internet users.

Chilling Effects on Legitimate Activities

Surveillance of peer-to-peer networks by copyright owners is intended primarily to find and monitor those who swap copyrighted content. However, since web bots are used by copyright owners to monitor an entire network, many other Internet users are inevitably caught in this web of surveillance, and legitimate file-sharing activities may be tracked. Peer-to-peer networks are not always used for downloading unauthorized content. For example, several sites of the peer-to-peer application BitTorrent offer legal content such as electronic music that is freely distributed by permission of the artists, videos of U.S. presidential debates and other political materials, and open-source software and freeware such as Linux.[86]

In *BMG Canada*, a public interest intervener submitted that if the court granted an order to disclose Internet users' identities on a low threshold test, then there could be a chilling effect on legitimate activities in cyberspace.[87] Some American commentators are also concerned that there may be chilling effects if courts readily order an ISP to turn over customer information to prying third parties, without first investigating whether copyright infringement has actually taken place.[88] If Internet users know that at any time an ISP could be required to expose their personal information, they may be reluctant to exercise legitimate uses of Internet applications.

Striking a Balance

As discussed above, copyright owners have a valid interest in defending their exclusive rights to control access to their products, but their current surveillance approach is eroding user privacy and alienating consumers rather than solving any problems of piracy.[89] If copyright owners' applications for disclosure of Internet users' personal information are too readily granted, intellectual property rights may be enforced at the undue expense of users' privacy rights. However, ISPs and the judiciary can play an important role in ensuring that privacy rights are fairly balanced against intellectual property rights.

The Role of ISPs

As gatekeepers between Internet users and the World Wide Web, ISPs have the technical ability to monitor and record their customers' activities in cyberspace, and to reveal their customers' identities and personal communications.[90] Anonymous Internet users are dependent on their ISPs to ensure that their identities remain concealed: "The current architectures of the networked world allow ISPs access to their users' personal information and private communications in a manner unparalleled by even the most powerful financial institutions or arms of government."[91]

The use and disclosure of account holders' personal information is governed by contract (the terms of the ISP's Internet services agreement) and statute (PIPEDA or the provincial equivalent).[92] Also, each ISP has a privacy policy ensuring some measure of privacy protection for their account holders.[93] Many Canadian ISPs are members of the Canadian Association of Internet Providers (CAIP)[94] and endorse the CAIP Privacy Code.[95]

While legislation and privacy policies generally guarantee some degree of privacy protection by controlling access to account holders' personal information, they do not go far in safeguarding account holders' procedural rights when their identities are being sought by third parties. In particular, there is currently no requirement for ISPs at law or under the CAIP Privacy Code to notify their account holders that third parties have made requests for disclosure of personal information. The Privacy Code simply states that "[a] member may notify users that an order has been received, if the law allows it".[96] Civil libertarian groups encourage ISPs to alert their account holders to requests for disclosure, in order to give those individuals an opportunity to retain counsel and anonymously challenge the request.[97] Some ISPs do in fact follow such a policy as a matter of fairness to their customers.[98]

The Federal Court and Federal Court of Appeal in *BMG Canada* did not comment on whether ISPs should notify their account holders. By contrast, a Pennsylvania District Court recently issued an order that took steps to protect the due process rights of alleged anonymous wrongdoers. As a result of the order, all ISPs in the Eastern District of Pennsylvania that are subpoenaed to disclose customers' personal information must first provide a detailed notice to their customers advising them of their rights and explaining how to challenge the subpoena.[99] ISPs in Canada could be required to follow a similar notice procedure to protect both the procedural and privacy rights of their account holders. This obligation is reasonable in light of the relationship between Internet users and ISPs. Ian Kerr suggests that because users increasingly depend on and trust their ISPs, in some circumstances users may be in a fiduciary relationship with their ISPs.[100] ISPs therefore may have fiduciary obligations to protect their customers' privacy that go beyond those currently required by contract or statute.

Recently proposed amendments to the *Copyright Act* may provide some measure of protection to alleged infringers by imposing obligations on ISPs.[101] Under the proposed legislation, a copyright owner may send to an ISP a notice of claimed infringement, which identifies

the claimant, the work or subject matter to which the claim of infringement relates, and the IP address of the alleged infringer. Upon receipt of the notice, the ISP is required to forward the notice to the alleged infringer and to retain records that would allow the identity of the alleged infringer to be determined.[102] As a result, Internet users who are the subject of these notices are alerted to potential copyright infringement proceedings. The proposed legislation, however, does not specify the procedures or requirements for disclosure of the records retained by the ISP. Thus, ISPs are still left with discretion in protecting the procedural and privacy rights of their customers.

The Role of the Judiciary

To date, there have only been a few cases where a party has asked a Canadian court to order an ISP to disclose the identity of an anonymous Internet user.[103] *BMG Canada* and *Irwin Toy* are the only of these cases that give any reasons.[104] As the Internet expands and surveillance correspondingly intensifies, it is expected that the number of these third-party discovery applications will increase. Thus, the judiciary will play an increasing role in protecting anonymous Internet users from spurious or uncertain claims based on unreliable evidence.

To protect Internet users' privacy interests, some measure of judicial oversight is required in applications to unmask anonymous Internet users. The Federal Court in *BMG Canada* enunciated a high threshold test that requires the applicant to establish a *prima facie* case against the alleged anonymous wrongdoer. However, the Federal Court of Appeal overturned this test and replaced it with the requirement that the applicant show a subjective *bona fide* belief of wrongdoing.[105] This lower threshold test is less protective of privacy interests. It could potentially lead to mistaken identification, since as *BMG Canada* illustrates, the process of identifying Internet users is highly problematic. Having a less stringent test could also result in the disclosure of the identities of individuals who have a clear defence against the allegations of wrongdoing.

Further, courts should consider applications for disclosure with a view to Charter values. Although the Charter can only be invoked to challenge state activities, as opposed to purely private activities, the common law must not develop inconsistently with Charter values.[106] The Supreme Court of Canada has held that privacy is worthy of constitutional protection under section 8 of the Charter (*i.e.* the right to be secure against unreasonable search or seizure).[107] However, section 8 guarantees only an individual's reasonable expectation of privacy in the circumstances. Courts have been more generous in finding that there is a reasonable expectation of privacy where the individual seeks to protect core biographical information that tends to reveal intimate details of the lifestyle and personal choices of the individual.[108] Disclosure of an Internet user's IP address, identity, and online activities could reveal highly personal information about his or her preferences and lifestyle that go beyond the scope of the copyright owners' allegations.[109] Anonymous Internet users thus have a reasonable expectation that their identities will not be revealed. To protect this expectation, courts should ensure that an order for disclosure is justified by clear and reliable evidence that the anonymous individual has infringed copyright.

The pre-litigation subpoenas issued under the U.S. *Digital Millennium Copyright Act* (DMCA)[110] demonstrate the dangers of having a broad discovery process with little judicial oversight and few due process considerations for an anonymous alleged wrongdoer. Section 512(*h*) of the DMCA permits a copyright owner to request a clerk to issue a subpoena to an ISP for identification of an alleged copyright infringer. This subpoena can be obtained fairly quickly and cheaply, as the only requirements are that the copyright owner must file a copy of notification, a proposed subpoena, and a sworn declaration that the information sought is for the sole purpose of protecting copyright.[111] Because of the lack of judicial supervision in the subpoena application process, several subpoenas have been mistakenly issued to reveal the identities of innocent individuals.[112] There are also several instances of abusive use of the subpoena powers where persons fabricated claims of infringement to expose another's identity and silence a particular expression.[113] As a result, many commentators have criticized the DMCA subpoena powers for encroaching on Internet users' freedom of speech and right to privacy.[114]

The use of the subpoena provisions was successfully challenged by an ISP in the *Verizon* case,[115] albeit on statutory grounds rather than on privacy or constitutional grounds. The RIAA had applied under the DMCA to compel Verizon to reveal the identities of Internet users who had allegedly swapped copyrighted songs over the file-sharing network Kazaa. The D.C. Circuit Court of Appeals found that based on a strict interpretation of the DMCA, section 512(*h*) subpoenas could not be issued against an ISP that was merely a conduit for the Internet users' acts of copyright infringement on peer-to-peer networks.[116] Verizon did not store the infringing material on its servers so it was acting only as a conduit for file-sharing. After this ruling, the RIAA could no longer use the subpoena provisions to obtain peer-to-peer users' customer information from ISPs. Instead, the RIAA initiated John Doe lawsuits against anonymous users identified only by their IP addresses, and subsequently used normal discovery-based procedures to determine the actual identities of the users.[117] John Doe actions provided greater procedural and substantive protections than the section 512(*h*) subpoenas because the RIAA was required to prove its case before a judge to some extent before obtaining the personal information. Alice Kao notes that after *Verizon*, the RIAA launched hundreds of John Doe actions and successfully applied

for orders to disclose customer's identities.[118] Thus, she argues that *Verizon* had little effect in enhancing the privacy of Internet users. The case only made it slightly more cumbersome for the RIAA to obtain the identities of Internet users.[119]

The Canadian legal system lacks provisions similar to the DMCA subpoena provisions. Rather, under the Federal Court Rules, the Federal Court has discretion to order a third party to disclose personal information about an alleged wrongdoer.[120] To guard against the concerns that were raised by the DMCA subpoenas, this discretion should not be exercised lightly by the court. If third party disclosure applications are carefully considered, using a fairly high threshold test and with a view to Charter values, anonymous Internet users will likely be protected against unfounded allegations of wrongdoing.

Conclusion

Peer-to-peer technologies have enabled millions of Internet users to access and exchange copyrighted content on an unprecedented scale. Copyright owners have responded by waging a battle against file-sharing that has little respect for privacy. They have set up automated systems to monitor and record file-sharing activities and scan through users' hard drives. Consequently, Internet users should not expect to be free from the watchful gaze of copyright owners.

Surveillance by private copyright owners is problematic because it is unclear how far they should be permitted to go in protecting their rights. Many Internet users do not expect their file-sharing activities to be tracked and monitored by copyright owners. Moreover, surveillance can lead to the inaccurate identification of wrongdoers, produce serious consequences for the individuals whose identities are revealed, and have a chilling effect on legitimate file-sharing activities.

One of the key protections that users have against online surveillance is anonymity. Anonymous Internet users can expect that their online activities will not be connected to their actual identities as long as their ISPs do not disclose customer-identifying information. Vigilant copyright owners, however, are seeking to compel ISPs to disclose the identities of customers who are trading copyrighted material over peer-to-peer networks. While the veil of anonymity should not be used to conceal illegal activity, it should also not be too readily lifted to allow copyright owners to pursue uncertain claims based on unreliable evidence. ISPs and the judiciary can play an important role in balancing an anonymous Internet user's right to privacy against a copyright owner's interest in unmasking the user.

Notes:

[1] E.J. Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" (1964) 39 N.Y.U.L. Rev. 962.

[2] R. Gavison, "Privacy and the Limits of Law" (1980) 89 Yale L.J. 421.

[3] J. Kang, "Information Privacy in Cyberspace Transactions" (1998) 50 Stan. L. Rev. 1193 at 1203.

[4] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 ["PIPEDA"].

[5] *Ibid.*, s. 2. Kang, *supra* note 3 at 1207, suggests that information can be identifiable to an individual if it is: (1) authored by the individual, (2) descriptive of the individual, or (3) instrumentally mapped to the individual. The first concerns information that an individual has created. The second concerns information that describes the status of an individual (such as name, address, sexual orientation, religion, health) or records discrete actions taken by an individual. The third concerns information that may be mapped to the individual for institutional identification (such as a social insurance number) or secured access or provision of services (such as a login name and password).

[6] PIPEDA, *supra* note 4, s. 3.

[7] *Ibid.*, s. 5 and Schedule 1. Pursuant to s. 5(1), organizations are required to comply with the obligations set out in Schedule 1. Schedule 1, Principle 3 states that "[t]he knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate".

[8] *Ibid.*, s. 7.

[9] "Application" refers to the software stored on each of the client and server machines that determines the type of Internet transaction and enables a two-way exchange of data between the client and server. Examples of applications are e-mail, file-sharing, Web browsers, multi-player computer games, and voice-over Internet protocol telephony. See C. McTaggart, "A Layered Approach to Internet Legal Analysis" (2003) 48 McGill L.J. 571 at 587–588.

[10] S. Katyal, "The New Surveillance" (2003) 54 Case W. Res. L. Rev. 297 at 311.

[11] *Ibid.*

[12] A. Colangelo, "Copyright Infringement in the Internet Era: The Challenge of MP3s" (2002) 39 Alta. L. Rev. 891 at 900.

[13] A. Pasick, "File-Sharing Network Thrives Beneath the Radar" *Livewire* (4 November 2004), online: <http://in.tech.yahoo.com/041103/137/2ho4i.html>.

[14] *United States v. Kennedy*, 81 F. Supp. 2d 1103 (D. Kan. 2000) [*Kennedy*]. Defendant was indicted for intentional receipt of child pornography and forfeiture after an anonymous Internet user tipped off the police that the defendant was sharing images of child pornography on a peer-to-peer network.

[15] L. Lessig, *Free Culture — How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity* (New York: Penguin, 2004) at 67.

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

[17] Katyal, *supra* note 10 at 340.

[18] *MGM Studios, Inc. v. Grokster Ltd.*, 380 F.3d 1154 (9th Cir. 2004).

[19] *MGM Studios, Inc. v. Grokster Ltd.*, 125 S. Ct. 2764 at 2770, 162 L. Ed. 2d 781 at 790 (Sup. Ct. 2005).

[20] Katyal, *supra* note 10 at 321.

[21] An ISP, or Internet Service Provider, is a communications provider that provides its account holders with Internet access and carries out the transmission of Internet traffic in response to account holders' commands. Major ISPs in Canada include Telus, Shaw, Bell, and Rogers. Also, most universities act as ISPs by providing Internet connectivity for faculty, staff and students.

[22] One does not have to be an account holder to access the Internet. See discussion under "Risks of Mistaken Identification" on page 174.

[23] A laboratory user study found that a majority of Kazaa users did not know what files they were sharing and sometimes assumed that they were not sharing any files when in fact they were sharing all files on their hard drive. The study suggests that some users were taking advantage of this by downloading files containing highly personal and private infor-

mation. See N.S. Good and A. Krekelberg, *Usability and Privacy: A Study of Kazaa P2P File-Sharing* (New York: ACM Press, 2003), online: <http://www.hpl.hp.com/shl/papers/kazaa/KazaaUsability.pdf>.

[24] R.W. Hubbard, P. DeFreitas, and S. Magotiaux, "The Internet — Expectations of Privacy in a New Context" (2001) 45 Crim. L.Q. 170 at 189. By analogy to a letter sent by "snail-mail", traffic data is like the information contained on the outside of the envelope.

[25] An IP address is a number that uniquely identifies a machine connected to the Internet. For example, the IP address of the Access Copyright Web site server on 27 September, 2005 was 209.171.63.4. This was determined by "pinging" the server at http://www.accesscopyright.ca.

[26] *Ibid.* at 189.

[27] *Ibid.* at 194.

[28] I. Kerr, "Personal Relationships in the Year 2000: Me and My ISP" in Law Commission of Canada, ed., *Personal Relationships of Dependence and Interdependence in Law* (Vancouver: UBC Press, 2002) 78 at 80.

[29] As of October 12, 2004, organizations in B.C. to which the *Personal Information Protection Act*, S.B.C. 2003, c. 63 [PIPA] applies are exempted from complying with PIPEDA. The federal government determined that the provincial PIPA is substantially similar to the federal PIPEDA. See *Organizations in the Province of British Columbia Exemptions Order*, S.O.R./2004-220.

[30] *In Re Verizon Internet Servs., Inc.*, 257 F.Supp. 2d 244, 267 (D.D.C. 2003). On appeal, the D.C. Circuit Court of Appeals did not comment on the privacy issues.

[31] *Kennedy*, *supra* note 14 at 1110.

[32] A. Kao, "RIAA v. Verizon: Applying the Subpoena Provision of the DMCA" (2004) 19 Berkeley Tech. L.J. 405 at 420.

[33] *Irwin Toy Ltd. v. Doe* (2000), 12 C.P.C. (5th) 103 (Ont. S.C.J.) [*Irwin Toy*].

[34] *Irwin Toy*, *supra* note 33 at paras. 10–11. This passage was also cited by Von Fickenstein J. in *BMG Canada*, FC, *infra* note 49 at para. 37.

[35] *Irwin Toy*, *supra* note 33 at para. 12.

[36] The ease with which Internet users can be tracked and monitored for wrongdoing results in greater enforcement and increases the impact of the law. Lessig, *supra* note 15 at 161, provides an interesting analogy for the constant surveillance of Internet users: "It is as if your car transmitted the speed at which you traveled at every moment that you drove; that would be just one step before the state started issuing tickets based upon the data you transmitted. That is, in effect, what is happening here."

[37] See *e.g.* Canadian Recording Industry Association, "Free Music Myth" (2000), online: <http://www.cria.ca/freemusicmyth.php>, describing the harms of downloading music and the "free music mentality".

[38] See CBC Online News Staff, "Studio Sues Movie Swappers" *CBC News Online* (16 November, 2004), online: <http://www.cbc.ca/story/arts/national/2004/11/16/Arts/moviesuits041116.html>, reporting that the Motion Picture Association of America initiated its first wave of lawsuits on November 16, 2004 against 200 to 300 individuals in the U.S. who were allegedly downloading movies illegally.

[39] Katyal, *supra* note 10 at 324–325.

[40] See *e.g. Society of Composers, Authors and Music Publishers of Canada v. Canadian Association of Internet Providers*, 2004 SCC 45; *Recording Industry Association of America, Inc. v. Verizon Internet Services, Inc.*, 351 F.3d 1229 (D.C. Cir. 2003) [*Verizon*, U.S. Court of Appeals].

[41] As of November 2004, more than 6,000 individuals have been sued in the U.S. by the Recording Industry Association of America for swapping MP3s over peer-to-peer networks. See K. Dean, "Movie Studios Sue File Traders" *Wired News* (16 November, 2004), online: <http://www.wired.com/news/digiwood/0,1412,65730,00.html>.

[42] Canadian Recording Industry Association, "Internet Piracy" (2000), online: <http://www.cria.ca/antipiracy.php>; Katyal, *supra* note 10 at 341.

[43] Katyal, *supra* note 10 at 341.

[44] *Ibid.*

[45] *Ibid.* at 340.

[46] Electronic Frontier Foundation lawyer Fred von Lohmann describes the invasion of privacy as "collateral damage" that arises whenever a very large percentage of the population is turned into lawbreakers. "If you're a copyright infringer, how can you hope to have any privacy rights? If you're a copyright infringer, how can you hope to be secure against seizures of your computer? How can you hope to continue to receive Internet access? . . . Well, what this campaign against file sharing has done is turn a remarkable percentage of the American Internet-using population into 'law-breakers' . . . And the consequence of this transformation of the American public into criminals is that it becomes trivial, as a matter of due process, to effectively erase much of the privacy most would presume." From Lessig, *supra* note 15 at 203 (quoting Fred von Lohmann).

[47] *Retail, Wholesale and Department Store Union, Local 580 v. Dolphin Delivery Ltd.*, [1986] 2 S.C.R. 573 at para. 39, *per* McIntyre J. [*Dolphin Delivery*].

[48] These restraints flow from a reasonable expectation of privacy guaranteed by s. 8 of the *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11. Section 8 is discussed in more detail below under "The Role of the Judiciary" at page 176.

[49] *BMG Canada v. John Doe*, 2004 FC 488 [*BMG Canada*, FC], aff'd 2005 FCA 193 [*BMG Canada*, FCA].

[50] Federal Court Rules, 1998, S.O.R./98-106, r. 233, 238.

[51] *BMG Canada*, FC, *supra* note 49 at para. 9.

[52] *Ibid.* at para. 13.

[53] *Ibid.* at paras. 16–20.

[54] *Ibid.* at paras. 21–29.

[55] *BMG Canada*, FCA, *supra* note 49 at para. 34.

[56] *Ibid.* at paras. 46–54.

[57] On August 25, 2002, the federal government released a consultation document proposing legislative amendments to provide law enforcement agencies with greater powers to investigate serious offences and threats to national security. See *Lawful Access Consultation Document* (Government of Canada: 2002), online: <http://canada.justice.gc.ca/en/cons/la_al/consultation_index.html>.

[58] See generally Colangelo, *supra* note 12.

[59] *Copyright Act*, R.S.C. 1985, c. C-42. See the fair dealing exceptions, ss. 29, 29.1 and 29.2, and private use exception, s. 80. See also Katyal, *supra* note 10 at 337.

[60] A 2001 study of the Internet habits of 5,682 Canadian youths (aged nine to 17 years) reported that 57% of youths found the playing and downloading of music to be one of their favourite Internet pastimes. Of the secondary students surveyed, 59% had downloaded MP3s, 30% had downloaded movies, and 20% had downloaded pirated software. See Environics Research Group, *Young Canadians in a Wired World: The Student's View* (prepared for the Media Awareness Network and Government of Canada, October 2001) at 15, online: <http://www.media-awareness.ca/english/resources/special_initiatives/survey_resources/students_survey/students_survey_report.cfm>.

[61] Lessig, *supra* note 15 at 67.

[62] *Ibid.* at 179. This characterization assumes that for every song downloaded there is one less song bought from a store.

[63] *Napster*, *supra* note 16 at 1013–1015.

[64] *BMG Canada*, FC, *supra* note 49 at paras. 25– 28.

[65] *Ibid.* at paras. 24–25.

[66] *Copyright Act*, R.S.C. 1985, c. C-42, s. 81.

[67] C. Schmitz, "Federal Court Rejects Bid to Track Web Music-Sharing" *The Lawyers Weekly* (16 April 2004) Vol. 23, No. 47. See also *Private Copying 2003-2004, Copying for Private Use* (a decision of the Copyright Board of Canada dated December 12, 2003) at 19–20, online: <http://www.cb-cda.gc.ca/decisions/c12122003-b.pdf>. Note that Howard Knopf's statement should be qualified: while making a copy of a sound recording onto audio recording media for private use does not constitute an infringement of copyright under s. 80 of the *Copyright Act*, this section does not legalize the online distribution of sound recording copies.

[68] *BMG Canada*, FCA, *supra* note 49 at paras. 46–54.

[69] It is estimated that 75% of music released by major labels is no longer in print. See Testimony of the Future of Music Coalition on "Online Entertainment and Copyright Law: Coming Soon to a Digital Device Near You" (submitted to the Senate Judiciary Committee, 3 April, 2001, 107th Cong., 1st sess.) at 4, online: <http://www.futureofmusic.org/images/FMC_testimony_4.3.01.pdf>.

[70] Lessig, *supra* note 15 at 68–69.

[71] *BMG Canada*, FC, *supra* note 49 at para. 20.

[72] *Ibid.* at para. 33

[73] *Ibid.*

[74] *Ibid.*

[75] *Ibid.* Matching account holders to IP addresses is an onerous, time-consuming task. Several employees of Rogers worked for four days to locate nine IP addresses. See *BMG Canada v. John Doe*, 2004 FC 488 (Written Representations of Rogers at paras. 8–10), online: <http://www.cippic.ca/en/projects-cases/file-sharing-lawsuits/Rogers_Written_Reps_Mar12.pdf>.

[76] *BMG Canada*, FC, *supra* note 49 at para. 34.

[77] *Ibid.* at para. 33. Telus, for example, has 750,000 individual Internet account holders and provides Internet service to 85,000 institutions, government departments, and corporations.

[78] *Ibid.* at para. 34.

[79] Note that individuals generally have to be the age of majority before they can be an account holder. Therefore it is possible that an account holder's child is responsible for the downloading activities. This raises interesting questions of accountability in light of para. 3 of the Telus Internet Services Account Agreement, which provides: "You are solely responsible and liable for any and all activities that occur under your account including, without limitation, all activities of any sub-account holders." Online: <http://www.mytelus.com/internet/policies/TISAA.do>.

[80] *BMG Canada v. John Doe*, 2004 FC 488 (Written Representations [of Telus] at para. 23), online: <http://www.cippic.ca/en/projects-cases/file-sharing-lawsuits/Written_Representations.pdf>. LANs can be set up by institutions, businesses, and residential households. There can be up to 255 computer users per LAN.

[81] *Ibid.* The practice of some Internet users who surf off their neighbour's unsecured wireless LAN, unknown to the neighbour, makes the identification of a user highly problematic.

[82] *BMG Canada v. John Doe*, 2004 FC 488 (Factum of the Intervener Canadian Internet Policy and Public Interest Clinic at para. 30), online: <http://www.cippic.ca/en/projects-cases/file-sharing-lawsuits/memorandum_fctd_final_12pt.pdf> [CIPPIC Factum].

[83] *Ibid.*

[84] *Copyright Act*, R.S. 1985, c. C-42, s. 38.1(1).

[85] *BMG Canada*, FC, *supra* note 49 at para. 3.

[86] Pasick, *supra* note 13.

[87] *BMG Canada v. John Doe*, 2005 FCA 193 (Factum of the Intervener Canadian Internet Policy and Public Interest Clinic at para. 31), online: <http://www.cippic.ca/en/projects-cases/file-sharing-lawsuits/CIPPIC%20FINAL%20Factum%20Aug%2010%202004.pdf>.

[88] See *e.g.* Katyal, *supra* note 10 at 365–366; Kao, *supra* note 32 at 421.

[89] Kao, *supra* note 32 at 426.

[90] McTaggart, *supra* note 9 at 609.

[91] Kerr, *supra* note 28 at 107.

[92] See under "Expectations of Privacy" at page 170.

[93] See *e.g.* Telus Privacy Code, online: <http://www.telus.com/privacy/download.html>; Shaw Privacy Policy, online: <http://secure.shaw.ca/policy/Privacy-Policy.html>.

[94] For a list of members, see Canadian Association of Internet Providers, online: <http://www.caip.ca/index2.htm>.

[95] CAIP Privacy Code, online: <http://www.caip.ca/issues/selfreg/privacy-code/privacy.htm>.

[96] *Ibid.*, Principle 5.

[97] J. Dolman, "When Can ISPs Be Compelled To Identify Their Customers? " *The Lawyers Weekly* (9 August, 2002), Vol. 22, No. 13.

[98] For example, Rogers in *BMG Canada* gave notices to their account holders who were affected by the application for disclosure: *BMG Canada v. John Doe*, 2004 FC 488 (Written Representations of Rogers at para. 12), online: <http://www.cippic.ca/en/projects-cases/file-sharing-lawsuits/Rogers_Written_Reps_Mar12.pdf>. See also D.L. Sobel, "The Process that 'John Doe' is Due: Addressing the Legal Challenge to Internet Anonymity" (2000) 5 Va. J.L. & Tech. 3. America Online notifies subscribers of subpoenas, while Yahoo complies with subpoenas without giving notice to subscribers.

[99] *Elektra Entertainment Group v. Does 1-6*, Civil Action No. 04-1241, 2004 U.S. Dist. LEXIS 22673 (D. Pa., 12 October 2004). For an article discussing this order, see K. Dean, "File Sharers Win More Protection" *Wired News* (28 October 2004), online: <http://www.wired.com/news/print/0,1294,65516,00.html>.

[100] Kerr, *supra* note 28 at 110.

[101] Bill C-60, *An Act to amend the Copyright Act*, 1st Session, 38th Parliament, 2005.

[102] *Ibid.*, s. 29.

[103] For a list of these cases, see *BMG Canada*, FC, *supra* note 49 at para. 41. In addition to these cases, there is *Philip Services Corp. v. John Doe* (1998), Court file no. 4582/98 (Ont. Ct. Gen. Div.), which according to Michael Geist was the first Canadian case to consider a motion to compel an ISP to disclose personal customer information. In that case, the Ontario Court, without giving any reasons, granted a motion to reveal the identity of Internet users who had made fraudulent postings to a stock chat room. See M. Geist, *Internet Law in Canada*, 3d ed. (Concord: Captus Press, 2002).

[104] *BMG Canada*, FC and FCA, *supra* note 49; *Irwin Toy*, *supra* note 33.

[105] *BMG Canada*, FCA, *supra* note 49 at para. 34.

[106] *Dolphin Delivery*, *supra* note 47 at para. 39.

[107] *R. v. Wise* [1992] 1 S.C.R. 527.

[108] See *R. v. Plant*, [1993] 3 S.C.R. 281 at para. 20 (pattern of electricity consumption is not core biographical information); *R. v. Tessling*, 2004 SCC 67 at para. 62 (heat radiating from a building is not core biographical information).

[109] CIPPIC Factum, *supra* note 82 at para. 18.

[110] *Digital Millennium Copyright Act*, 17 U.S.C. §512(*h*) (1998).

[111] *Ibid.*

[112] See Kao, *supra* note 32 at 423–424.

[113] *Ibid.* at 422–423; Katyal, *supra* note 10 at 369.

[114] See *e.g.* Katyal, *supra* note 10 at 367–368.

[115] *Verizon*, U.S. Court of Appeals, *supra* note 40.

[116] *Ibid.* at 1237.

[117] Kao, *supra* note 32 at 418.

[118] *Ibid.* at 427.

[119] *Ibid.*

[120] See note 50, *supra*.