Contours of Privacy

Contours of Privacy

Edited by

David Matheson

CAMBRIDGE SCHOLARS PUBLISHING

Contours of Privacy, Edited by David Matheson

This book first published 2009

Cambridge Scholars Publishing

12 Back Chapman Street, Newcastle upon Tyne, NE6 2XX, UK

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN (10): 1-4438-0106-2, ISBN (13): 978-1-4438-0106-5

TABLE OF CONTENTS

Part III: Privacy and the Mind

Part IV: Privacy and Emerging Technologies

INTRODUCTION

EXPLORING THE CONTOURS OF PRIVACY

DAVID MATHESON

"Perhaps the most striking thing about the right to privacy," the American ethicist Judith Jarvis Thomson once remarked, "is that nobody seems to have any very clear idea what it is" (Thomson 1975, 295). She went on to suggest that there is a good reason for the lack of clarity. The concept of privacy itself, she argued, doesn't really pick out a single, unified interest across the various contexts in which we apply it. Rather, it refers to a variety of interests that have little in common outside of the fact that they happen to collected under a single term. And it's hard to be clear about what the interest is to which the right to privacy entitles us when that interest is by its very nature disjointed.

Even in more integrative accounts of privacy, however, explanations of the lack of clarity are not hard to come by. Consider, for example, the well-known limited access account of privacy as articulated by Ruth Gavison (1980) and Anita L. Allen (1989), according to which privacy amounts to the condition of having others' access to one's person limited in important ways. Here, the concept of privacy is taken to refer to a unified interest—the condition of limited access—across the various contexts in which we properly apply it. But that interest is general, and it may take many different particular forms in the different contexts, depending on the sorts of access salient in those contexts. Where the access under consideration is spatial, the privacy interest might take the form of solitude, seclusion, or property concerns; where the access is knowledge-related, it might take the form of the protection of personal information; and so on. Or consider the ignorance account of privacy proposed in the work of William Parent (1983a & 1983b). In this account, the concept of privacy again refers to a unified, general interest in whatever context in which we properly apply it, *viz*., the ignorance of others with respect to one's publicly undocumented personal information. Even here, privacy would seem to come in many particular forms, each

distinguished from the others by means of the particular sort of personal information, and hence the particular sort of ignorance, that is in focus. Health privacy, for example, might be said to pertain to others' ignorance of one's medical information; decisional privacy might be cashed out as others' ignorance of information about one's intimate decisions; and physical privacy might be understood as involving others' ignorance of sensitive details about one's present physical appearance, activity, or possessions. Moreover the reason why privacy is valued—what renders it an interest—will presumably vary along with its particular form in different contexts. With so many potential forms of, and interests comprehended under, privacy, it would be surprising if there *weren't* a good deal of uncertainty about just what the right to privacy involves.

Whether we adopt a disjointed or integrative account, then, the upshot seems to be that the contours of privacy are bound to be varied and numerous. This book represents an effort by an international and multidisciplinary group of scholars to limn the variegated contours of privacy—to explore its many forms and our many reasons for valuing it (positively or negatively)—in different contexts. The origin of many of the contributions here presented was an international Contours of Privacy Conference held at Carleton University (Ottawa, Canada) in November of 2005, which was sponsored by the Social Sciences and Humanities Research Council of Canada research project, *On the Identity Trail: Understanding the Importance and Impact of Anonymity and Authentication in a Networked Society* (www.anonequity.org), the Centre on Values and Ethics at Carleton University (www.carleton.ca/cove), and the Sheldon Chumir Foundation for Ethics in Leadership (www.chumirethicsfoundation.ca). The success of the conference inspired speakers and audience members to request a volume in which contributions were collected. Happily, Cambridge Scholars Publishing has met that request in a most satisfactory way.

The first section of the book focuses on the relationship between privacy and anonymity, on the one hand, and accountability on the other. Healthy participation in society involves some degree of accountability to others. On the face of things, however, accountability does not fit well with privacy and anonymity, and a discussion of the apparent lack of fit is important for a deeper understanding of the positive and negative value to be attached to privacy in social and political contexts. Ian Kerr and Alex Cameron's contribution contains an illuminating discussion of one contemporary way in which the encroachment upon privacy and anonymity in the putative interest of accountability threatens to undermine healthy social participation. They explore the reasons behind a Canadian

Federal Court's refusal to compel Internet service providers to disclose the identities of subscribers alleged to have been engaged in unlawful peer-to-peer file sharing. In view of the very real danger that the Court's decision could have the ironic effect of encouraging more powerful private-sector surveillance of our on-line activities for less-than-admirable ends, Kerr and Cameron argue, there is a call for the Court to continue to develop its understanding of the conditions under which the compelled disclosure of identity is legitimate, with special consideration being given to a broad-based public interest in privacy.

Hugh Hunter aims to shed light on privacy and accountability by taking us back in the history of Western philosophy. On one ancient account derived from Xenophon, ubiquitous accountability to others—and hence a pervasive lack of privacy—is thought to be an important ingredient in citizens' motivation for healthy—virtuous—social life. Where the panopticism that this account seems to imply is managed in such as way as to be rendered consistent with Socratic insights about the connection between self-knowledge and virtue, Hunter suggests, it may be more conducive to broadly social flourishing than one might suppose upon first consideration.

Privacy and anonymity are often mentioned in the same breath, a fact that underscores the common assumption that anonymity is one of the central kinds of privacy. But in what sense does anonymity stand as an especially valuable element of privacy? And are there important kinds of privacy that anonymity does not guarantee? In her opening contribution to the second section of the book, Marsha Hanen addresses the first of these questions by considering the place of anonymity (and the complementary concept of social identity) within some prominent contemporary approaches to privacy, and through the lens of feminist theories of knowledge that highlight the various contextual parameters within which anonymity gains its meaningfulness. In his contribution, Travis Dumsday answers the second question affirmatively by drawing our attention to cases in which there is a very real sense of privacy loss despite the presence of anonymity—cases in which the contours of privacy seem to stretch well beyond anonymity. He goes on to highlight some possible solutions to the ethical worries surrounding privacy loss in such contexts as anonymized medical information.

The case studies that Catarina Frois presents nicely illustrate the various ways in which the possession of anonymity can serve as an instrument for the salutary relinquishment of other forms of privacy by members of organizations such as Alcoholics Anonymous. Thus, not only are there forms of privacy beyond anonymity, the very value of anonymity

might derive at least in part from its capacity to encourage the abandonment of privacy in other ways.

Inquiring minds want to know, we are told, and what they want to know frequently lies within the bounds of the private. This raises interesting issues about privacy and the human mind that Aritha van Herk, Stephen Margulis, and Steven Davis take up in the book's third section. One such issue concerns the origin of the widespread desire to know. Why are the details of private lives so coveted in our society, especially when a professed concern for privacy is so prevalent? Van Herk's exploration—delivered in the deeply engaging way that one would expect of such an accomplished literary figure—suggests that the desire might be rooted in a misguided conviction about the extent to which watching others reveal the most private parts of their lives will assist us in validating our own. The social milieu in which privacy is commodified and its relinquishment viewed as a harmless diversion, she argues, serves only to deepen the conviction.

A related issue concerns the psychological character of privacy, along with the sorts of psychological effects that its possession or loss might entail. Margulis contends that the psychological character of privacy (as the concept is typically used in the behavioral sciences) is best seen through the lens of a variation on the limited access account of privacy found in the work of Alan Westin (1967) and Irwin Altman (1975), where the focus is on the individual's own control over others' means of access to her. As for the psychological effects of privacy's possession and loss, Margulis points out that the empirical evidence is at present relatively lacking and unevenly distributed across privacy issues, leaving us to speculate about those effects on the basis of indirect behavioral considerations.

Davis's carefully constructed account of privacy throws its psychological character into stark relief. In this account, not only does privacy entail the absence of certain psychological states in others with respect to one's personal information; it further implies the presence of affective attitudes about such information in one's society, and promotes various moral values—respect, dignity, and love, for example—that are themselves deeply psychological in nature.

The final section of the book concerns what Langdon Winner (1986) might call the privacy "politics" of emerging information technologies. Artifacts in general have teleological features—politics—built right in: what they are cannot be understood apart from the goals they are designed to achieve. The same applies to recent information technologies. In what ways do the teleological features of these technologies pose a threat to the

privacy of users? How sensitive should the design of the technologies be to the interests of privacy? In her captivating contribution, Valerie Steeves makes a compelling case that the supposedly privacy-respecting politics of such online networking sites as Facebook.com may be constructed on false assumptions about the extent to which large segments of users—children—are voluntarily exposing information about themselves therein. Ralph Gross and Alessandro Acquisti suggest that users of such networking technologies are not so much irrational in their privacy preferences as they are unaware of the heavy privacy cost carried by certain relational features of the systems, such as the actual boundaries of the online communities with which they are connected.

Michael Zimmer draws our attention in a similar fashion to the significance of new vehicle communication technologies, and suggests that there is a much greater need for more widespread discussion of the privacy effects of these technologies, and for an elevated sensitivity to their privacy politics by those involved in their design.

Krista Boa concludes by highlighting the ways in which a failure fully to appreciate the privacy politics of emerging information technologies has generated negative consequences in the Supreme Court of Canada's handling of the reasonable expectation of privacy in public spaces. Public spaces may be ones in which there is no reasonable expectation to be free from being observed. But this does not imply that they are spaces in which there is no reasonable expectation to be free from being watched or monitored, Boa points out; and it is just such monitoring, in contrast to mere observation, that enhanced information technologies deployed in pubic spaces tend to promote. The Supreme Court's decisions about the reasonable expectation of privacy, she argues, fail fully to appreciate these facts.

References

Allen, A.L. 1989. *Uneasy access: Privacy for women in a free society*. Totowa, NJ: Rowman & Littlefield.

Altman, I. 1975. *The environment and social behavior: Privacy, personal space, territory, and crowding*. Monterey, CA: Brooks/Cole.

Gavison, R. 1980. Privacy and the limits of law. *Yale Law Journal* 89, 421-71.

Parent, W. 1983a. A new definition of privacy for the law. *Law and Philosophy* 2, 305-38.

—. 1983b. Privacy, morality, and the law. *Philosophy & Public Affairs* 12, 269-88.

Thomson, J.J. 1975. The right to privacy. *Philosophy & Public Affairs* 4, 295-314.

Westin, A.L. 1967. *Privacy and freedom*. New York: Atheneum.

Winner, L. 1986. Do artifacts have politics? In L. Winner, *The whale and the reactor: A search for limits in an age of high technology*, 19-39. Chicago: University of Chicago Press.

PART I:

PRIVACY, ANONYMITY AND ACCOUNTABILITY

CHAPTER ONE

SCOPING ANONYMITY IN CASES OF COMPELLED DISCLOSURE OF IDENTITY: LESSONS FROM *BMG V. DOE*[*]

IAN KERR[**] AND ALEX CAMERON[***]

I. Introduction

Some people go online to share music—to explore the limits of their imaginations, to discover songs from various musical genres and to feel the beat of previous generations. In the U.S., sharing music across some

---

[*] This chapter is adapted from I. Kerr & A. Cameron, "Nyms, P2P & ISPs," in K.J. Strandburg & D.S. Raicu, eds., *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation*, (New York: Springer, 2005), 269-94, by permission of the authors. 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 Meghan Murtha for her keen eye and her excellent research assistance and to Professors Jane Bailey, Michael Geist, and Philippa Lawson for their very helpful comments, which resulted in a much better chapter. Finally, congratulations to 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 where this project was first presented and for publishing an excellent book out of that symposium, where the earlier version of this chapter was first published.

[**] 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 chapter derives: *On the Identity Trail: Understanding the Importance and Impact of Anonymity and Authentication in a Networked Society* (www.anonequity.org).

[***] 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.

peer-to-peer (P2P) networks is illegal (*A&M Records v. Napster*). In Canada, it is not. Not yet (*BMG v. Doe*, para. 54[1]).

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. Individuals can use nyms to access and explore a wide variety of online materials that may help shape their identities, including books, films and music, for example. In the U.S., this form of personal exploration has been affected by litigation campaigns that have successfully sought to compel Internet service providers (ISPs) to disclose their customers' offline identities to copyright holders (Jean 2004).[2] In Canada, such campaigns have not enjoyed the same success. Not yet.[3]

Why did Canada's Federal Court and Federal Court of Appeal 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? How did the court contour anonymity interests against copyright holders' interests? Should the decision be followed in other cases? What can be learned from this decision?

This chapter aims to address these 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.

II. Anonymity

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 (Froomkin 2003 and, generally, Marx 1998). Anonymity is like the Duke's toad in Shakespeare's *As You Like It*—ugly and venomous, and yet it wears a precious jewel in its head.

Ugly and venomous, because it disables accountability and enables wrongdoing. In the P2P context, an inability to ascertain the real-life

---

[1] Expressly refusing to rule on the copyright infringement claims one way or another.

[2] In fact, in the United States, not every attempt to compel subscriber identities from ISPs has proven successful. Some courts have shown that subscriber identities should not be handed over too easily. See, *e.g.*, *RIAA v. Verizon.*

[3] It is important to note, however, that Canadian courts regularly order individuals' online identities to be revealed in other specific contexts, for example, online defamation. See, *e.g., Vic Alboini & Northern Financial v. Doe*, per C. Campbell J (ordering a website host and Internet service providers to disclose information in an Internet defamation case).

identities of *geekboy@KaZaA, mr_socks@KaZaA, chickiepoo25@KaZaA*[4] 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.

If P2P networks were perfectly anonymous, copyright industries would have no means of legal recourse against individuals accused of copyright infringement. As Professor Lawrence Lessig once remarked, in its broader context, "[p]erfect anonymity makes perfect crime possible" (Lessig 1995, 1750; cf. Froomkin 1995, para. 46). 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 perfectly anonymous P2P networks.

Though dangerous, anonymity is at the same time precious. It is Plato's *pharmakon* (Derrida 1981); 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" (Derrida 1981, 70). 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" (Clark 2004). 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 (Marx 1998). Nyms can be used to enhance privacy by controlling the 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" (Marx 1998).

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 (see Biddle *et al.* 2002; Clarke; du Pont 2001; Zarsky 2004), 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—perfect anonymity is usually not possible online.

[4] These are some of the nyms at issue in *BMG v. Doe*.

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, as in other cases where parties wish to identify Internet users, finding out the IP address of a 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; at least not without help from a third party intermediary. In this case, the ISPs were the targeted intermediaries and they 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.

ISPs have increasingly become trusted holders of and gatekeepers to our personal information. ISPs 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 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 (Kerr 2001 & 2002). 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 (*SOCAN v. CAIP*, para. 155 [LeBel, J., dissenting.]).[5]

[5] See also *Irwin v. Doe*, paras. 10-11.

In *BMG v. Doe*, Canada's Federal Court and the Federal Court of Appeal were 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). *BMG v. Doe* is an important comparative IP and cyberlaw case because it forces courts to consider a judicial test for determining when ISPs should be compelled to disclose their customers' identities to copyright owners.

III. *BMG v. Doe*

On March 31, 2004, the Federal Court 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 (Borland 2004b & 2004c; Smith 2004; Koprowshi 2004). The media coverage 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.

On appeal in 2005, the Federal Court of Appeal upheld the lower court ruling, though it modified it somewhat and downplayed the lower court's comments regarding copyright law. Although the appellate ruling lowered the threshold on one aspect of the test for disclosure of identities, other aspects of the ruling may effectively have raised the level of privacy protection afforded to online nyms.

BMG v. Doe is significant because it may have set the threshold test for future cases in Canada and perhaps elsewhere, in which courts are asked to compel ISPs to link individuals' online nyms—specifically their IP addresses—to their offline identities.

A. 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").[6]

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 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.

1. Evidence

a. CRIA's evidence

The bulk of CRIA's evidence in support of the Motion came from Mr. Millin, the President of 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,[7] MediaSentry was then able to determine to which ISPs the IP addresses had been assigned at the relevant times. This allowed MediaSentry to determine the ISP through which each Defendant had been sharing the files.

---

[6] 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*.

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

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. MediaDecoys are files that appear, based on their filenames, to be copyrighted songs. However, once a P2P user downloads and opens such a file, the user discovers 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.

b. 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 an event and Telus's 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 hearing. Finally, Telus provided evidence about how responding to CRIA requests would be costly and disruptive to Telus's 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. Privacy arguments in *BMG v. Doe*[8]

a. 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:

i. Is there a *prima facie*, or *bona fide* case, at least, of copyright infringement?
ii. Is there a relationship between the ISPs and the alleged infringers?
iii. Do the ISPs have information about the identities of the alleged infringers?
iv. Are the ISPs the only practical source of the information sought?
v. Is the information necessary for CRIA to proceed with its lawsuit?
vi. Would the information sought be compellable at trial and useful to CRIA's case?

[8] This section primarily discusses the privacy arguments advanced before the lower court. The arguments before the appellate court were largely the same, though advanced in the context of alleging that the lower court had either erred or not erred. Complete 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.

vii. 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 (*Personal Information Protection and Electronic Documents Act*, ss. 7(3)(c)). 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 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.

b. 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's 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.

c. 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 values included protection of informational privacy which the Supreme Court had expressly recognized in Canada (*R. v. Dyment*, paras. 427-30). In explaining why the threshold test was critical from a privacy perspective, CIPPIC pointed to *R. v. Dyment* where the Supreme Court of Canada 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" (*R. v. Dyment*, paras. 429-30).

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 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 (CIPPIC 2004a, para. 17-18).

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 types of files. 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. This point was later specifically embraced by the Federal Court of Appeal, which held that the investigation by CRIA must be limited to relevant information only.[9]

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 U.S., 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.

3. The Federal Court decision

The Federal 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-Goldwyn-Mayer v. Grokster*. 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?"

[9] See discussion *infra* section III.A.4 of this chapter.

a. What legal test should the Court apply before ordering disclosure?

Justice von Finckenstein of the Federal Court held that the following five criteria must be satisfied before a disclosure order would be made:

i. The Plaintiff must establish a *prima facie* case against the Defendants;
ii. The ISPs must be in some way involved in the matter under dispute (*i.e.* the ISPs must be more than innocent bystanders);
iii. The ISPs must be the only practical source of the information;
iv. The ISPs must be reasonably compensated for their expenses arising out of compliance with the order, in addition to their legal costs; and
v. 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, on what we characterize as *a broader public interest in privacy*, as discussed below in Part IV.

b. 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 in disclosure. The Court's analysis followed each factor of the threshold test as follows.[10]

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 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" (*BMG v. Doe*, para. 19).

Second, the Court noted that Millin had not explained how MediaSentry linked the P2P pseudonyms to specific IP addresses.

[10] The Court offered most of its analysis in *BMG v. Doe* between paras. 10-42.

Therefore, the Court concluded that it would be "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 (*BMG v. Doe*, para. 20).

Finally, Justice von Finckenstein found that CRIA had not provided any evidence that copyright infringement had taken place under Canadian law.

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 the view that there is a legal relationship between ISPs and those who use their services; a relationship which may create privacy-related obligations that are not applicable to innocent bystanders.

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's 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" (*BMG v. Doe*, para. 36). 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 (*BMG v. Doe*, para. 37; quoting *Irwin v. Doe*, paras. 10-11).

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 one individual's privacy rights against the rights of other individuals and 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 the alleged wrongdoers (*BMG v. Doe*, para. 42). 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 (*BMG v. Doe*, para. 42). 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* (*BMG v. Doe*, para. 42; emphasis added).

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 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.

c. 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 restrictions would have been needed to protect the privacy of the Defendants because "the invasion of privacy should always be as limited as possible" (*BMG v. Doe*, para. 44).

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, the P2P pseudonyms would be used as proxies 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 be required to disclose only the name and last known address of each account holder. These kinds of protections would provide the information CRIA needed to proceed with a given claim while, at the same time, provide a measure of privacy protection to Defendants.

4. The Federal Court of Appeal decision

The Federal Court of Appeal upheld the decision of the lower court, with some modification. Like the lower court, the appeals court began its decision by affirming the significance of individuals' online privacy concerns in our modern information society: