



OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
— for —
British Columbia

Balancing Privacy & Openness: Internet Publication of Tribunal Decisions¹

David Loukidelis²

Information and Privacy Commissioner for British Columbia

Beyond the Horizon: The Expanding and Overlapping Jurisdiction of Arbitrators & Tribunals

Canadian Bar Association, Administrative Law Presentation

September 22, 2009

Canadian Bar Association, Edmonton, Alberta

INTRODUCTION

The Supreme Court of Canada has often affirmed the vital importance of the open court principle, which has been described as the “palladium of liberty”.³ The open court principle holds that court proceedings should be a matter of public record, so that justice is both done and is seen to be done⁴. Although this principle does not appear to apply to administrative tribunals in the same way as

¹ This is a version of a paper the author originally presented in November 2008 to the CBA’s National Conference on Administrative Law, in Ottawa.

² I am very grateful to my colleague, Caitlin Lemiski, for her indispensable research and writing contributions to this paper.

³ *Millward v. Canada (Public Service Commission)*, [1974] F.C.J. No. 161, at para. 40.

⁴ See, for example, *Named Person v. Vancouver Sun*, 2007 SCC 43, [2007] S.C.J. No. 43, and *Canadian Broadcasting Corp. v. New Brunswick (Attorney General)*, [1996] 3 S.C.R. 480.

it does to courts, it is surely uncontroversial to argue that tribunal proceedings also should be open, not only to the parties, but to the public.⁵

At the same time, the need to protect personal information in published tribunal decisions has been heightened in recent years because of how the internet has increased public access to justice information. Today, anyone can go online and find legislation and court decisions simply and quickly, very often for free. This is highly desirable for a number of reasons. This advances the cause of openness. Online access improves access to justice, fosters public understanding of the law and increases transparency and accountability of public authorities. Administrative tribunals have been part of this trend since, like the courts, many publish their decisions online.

Many commentators have noted that internet publication of decisions—indeed, any publication of decisions—creates tension between two competing values, an open and accessible justice system and the right to privacy. Questions arise about protecting the personal information of individuals involved in court and tribunal processes while continuing to foster openness and accountability. This paper addresses these questions in relation to the disclosure in tribunal decisions⁶ of personal information of parties, as well as witnesses and other third parties.⁷

Without attempting to be an exhaustive or scholarly piece, this paper examines how Canadian privacy laws affect disclosure of personal information through publication of tribunal decisions and suggests steps to protect privacy while promoting transparency and accountability in decision-making. This paper's

⁵ D. Jones & A. S. de Villars, *Principles of Administrative Law*, 4th ed. Thomson Carswell, at p. 296. The authors acknowledge, however, that the question of “[t]he openness of judicial proceedings becomes more difficult where the nature of the administrative proceedings leans more towards a judicial model” (p. 296).

⁶ Questions arise, of course, about privacy of personal information in files for tribunal proceedings, just as they have arisen in the context of access to records in court files, particularly online files. These issues are not addressed here.

⁷ This paper addresses the privacy of “personal information”, meaning information about identifiable individuals. It does not address confidentiality claims respecting information of or about organizations, including business corporations, caught up in tribunal proceedings and decisions.

essential argument is that, leaving aside what privacy laws require of them, tribunals can and should both respect the open court principle and protect personal information of those involved in their processes.

OPEN COURTS, OPEN TRIBUNALS

The Supreme Court of Canada has observed that

...the more complex society becomes, the more important becomes the function of the courts. As a result of their significance, the courts must be open to public scrutiny and to public criticism of their operation by the public.⁸

The role of tribunals in our increasingly complex society is vital and their decisions can have a significant impact on the rights and interests of those appearing before them. Regardless of whether the open court principle technically applies to tribunals, it is surely uncontroversial to suggest that tribunals should wherever possible adopt, as a matter of policy, the principle of openness.

At the same time, developing concepts of the duty to give reasons for decision, and of the functions of reasons, favour more openness and transparency in the operation of Canadian courts and, by extension, of administrative tribunals. The Supreme Court of Canada made it clear in *Baker v. Canada (Minister of Citizenship and Immigration)*⁹ that, as a matter of fairness, there is some duty for administrative decision-makers to give reasons. *Baker* indicates that, “where the decision has important significance for the individual, when there is a statutory right of appeal, or in other circumstances, some form of reasons should be required”.¹⁰

⁸ *Edmonton Journal v. Alberta (Attorney General)*, [1989] 2 S.C.R. 1326, at para. 5 (online at: <http://csc.lexum.umontreal.ca/en/1989/1989rcs2-1326/1989rcs2-1326.html>).

⁹ [1999] 2 S.C.R. 817 (online at: <http://csc.lexum.umontreal.ca/en/1999/1999rcs2-817/1999rcs2-817.html>).

¹⁰ *Baker*, at para. 43.

The Supreme Court of Canada has also recently considered the function of reasons for decision, albeit in the criminal and not administrative law context.¹¹ McLachlin C.J.C. observed that reasons for decision serve three functions: to tell the parties affected by the decision why the decision was made, to provide public accountability so that justice is not only done, but is seen to be done, and to permit effective appellate review.¹²

THE “CONSTELLATION OF INTRUSIONS”¹³

Academics have weighed in with concerns about the threat to individual privacy created by online posting of even seemingly innocuous information, leading to what Helen Nissenbaum has termed “the problem of privacy in public.”¹⁴ She noted that, to many, “the idea that privacy may be violated in public has an oddly paradoxical ring”, but she argues that personal information, taken out of context, violates the privacy interests of individuals in a fundamental way:

Most people have a robust sense of the information about them that is relevant, appropriate, or proper to particular circumstances, situations, or relationships. When information is judged appropriate for a particular situation it usually is readily shared; when appropriate information is recorded and applied appropriately to a particular circumstance it draws no objection. People do not object to providing to doctors, for example, the details of their physical condition, discussing their children's problems with their children's teachers, divulging financial information to loan officers at banks, sharing with close friends the details of their romantic relationships. For the myriad transactions, situations and relationships in which people engage, there are norms—explicit and implicit—governing how much information and what type of information is fitting for them. Where these

¹¹ *R. v. R.E.M.*, 2008 SCC 51, [2008] S.C.J. No. 52 (online at: <http://csc.lexum.umontreal.ca/en/2008/2008scc51/2008scc51.html>).

¹² Para. 11.

¹³ Helen Nissenbaum, “Protecting Privacy in an Information Age: The Problem of Privacy in Public”, *Law and Philosophy*, 17: 559-596, 1998 at p. 31 (online at: <http://www.nyu.edu/projects/nissenbaum/papers/privacy.pdf>).

¹⁴ Nissenbaum, note 7, at p. 2.

norms are respected I will say that contextual integrity is maintained; where violated, I will say that contextual integrity has been violated.¹⁵

In both the judicial and administrative tribunal contexts, online publication of justice system information can have serious privacy consequences. The court clerk for an Ohio county posted full-text versions of a wide variety of court documents online, later saying he didn't realize that by doing so he was "walking into a privacy hornet's nest".¹⁶ In one instance, an individual used a social security number, birth date and signature obtained online to create a fake identity and open credit cards under a false name. Real estate buyers were able to check sellers to see whether a divorce or other legal troubles might be a reason for the sellers to sell.

This article offers only a few examples of the kinds of privacy-related risks that can be triggered when the "practical obscurity"¹⁷ of paper records is supplanted by online publication. Some have identified the risk that sexual predators could use personal information posted online to identify and then target children of recently divorced parents.¹⁸

In the United States, where the courts have found a common law right "to inspect and copy public records and documents, including judicial records and documents",¹⁹ one report described the privacy risks this way:

For instance, the commercial sector can analyze court or corrections data to determine which heads of households have been incarcerated and use this data to market targeted services or products to the offenders' families,

¹⁵ Nissenbaum, note 7, at p. 20.

¹⁶ Jennifer Lee, "Dirty Laundry, Online for All to See", *The New York Times*, September 5, 2002 (online at: <http://query.nytimes.com/gst/fullpage.html?res=9A04E4D9173EF936A3575AC0A9649C8B63>).

¹⁷ See *Department of Justice v. Reporters Committee*, 489 U.S. 749 (1989) (online at: <http://supreme.justia.com/us/489/749/case.html>).

¹⁸ "Submission on the Discussion Paper: *Open Courts, Electronic Access to Court records, and Privacy*", Canadian Bar Association, April 2004 (online at: <http://www.cba.org/CBA/submissions/pdf/04-13-eng.pdf>).

¹⁹ See *Nixon v. Warner Communications, Inc.*, 435 U.S. 589 (1978), at p. 597, as quoted by Cory J. in *Edmonton Journal v. Alberta (Attorney General)* [1989] 2 S.C.R. 1326 at para. 7 (online at <http://csc.lexum.umontreal.ca/en/1989/1989rcs2-1326/1989rcs2-1326.html>).

such as security systems, credit cards, and home equity loans. In another example, bulk data could be analyzed to isolate names of victims or family members and do targeted marketing on services or products. Picture a rape victim being inundated by junk mail for stress relievers, women's magazines, counselling, self-defence programs, athletic equipment, and even gun stores. Sound a bit unpalatable? Unfortunately, it is not far from reality.²⁰

The Canadian Judicial Council ("CJC") has framed the challenge of online information in this way:

The "practical obscurity" fostered by paper-based records has meant that records were difficult and costly to obtain, search, and link with other documents. This has meant that purposes unconnected with the accountability of the judicial system, and which could have a serious negative impact on other constitutional values, have largely not been pursued by members of the public. However, the move towards a digital environment brings such possibilities to the fore. Furthermore, the digital environment permits the linking and aggregation of personal information, which can make privacy and security concerns stronger than in a paper-based environment.²¹

This is not a merely hypothetical concern in Canada. The practical impact of the tension between openness and privacy is illustrated in *Alberta (Attorney General) v. Krushell*.²² An individual had requested a copy of a list of the names of accused individuals found in each Alberta criminal court docket between 1990 and 2005. He apparently hoped to sell the information on the internet. In holding that the

²⁰ Recommendations of the Minnesota Supreme Court Advisory Committee on Rules of Public Access to Records of the Judicial Branch" (June 2004) (online at: <http://www.lawlibrary.state.mn.us/access/accessreport.htm>), quoting from the National Criminal Justice Association privacy guideline, "Developing, Drafting and Assessing Privacy Policy for Justice Information Systems" (online at <http://www.ncja.org/Content/NavigationMenu/PoliciesPractices/JusticeInformationPrivacyGuideline/privacyguideline.pdf>).

²¹ Canadian Judicial Council, "Model Policy for Access to Court Records in Canada" (2003), at paras. 19 & 20 (online at: http://www.cjc-ccm.gc.ca/cmslib/general/news_pub_techissues_AccessPolicy_2005_en.pdf).

²² *Alberta (Attorney General) v. Krushell*, 2003 ABQB 252 (online at: http://foip.alberta.ca/commissioners_decisions/other/judicial_reviews/pdf/JRF2002-022.pdf).

requested records were not covered by Alberta's freedom of information law, Bielby J. said the following about posting such information online:

The mischief which could be created by allowing ready public access to the names of unconvicted accused is not difficult to imagine. Statutorily prescribed punishments for the convicted would pale in many cases in comparison to the de facto punishment created by posting information on the criminally charged for the benefit of the gossip and the busybody. Similarity of names might create defamatory impressions. Same-day internet postings would create concern about courthouse security and judge-shopping which could affect the administration of justice and thus judicial independence in ways the Legislature clearly attempted to avoid by so carefully exempting all matters relating to the judiciary in other subsections of s. 4 [of the *Alberta Freedom of Information and Protection of Privacy Act*]. ... While there is currently limited public access to this information via the physical daily posting of the criminal dockets on site, that does not justify posting world-wide for all time to all of those with access to the internet.²³

Another striking example comes from Saskatchewan. In 2005, Saskatchewan's Information and Privacy Commissioner, Gary Dickson, Q.C., investigated a complaint by an individual against that province's Automobile Injury Appeal Commission ("AIAC").²⁴ The AIAC had begun posting decisions on its website that contained applicants' first and last names, as well as personal medical information and detailed financial information. The AIAC tried to justify its practice relying in part on the open court principle. Commissioner Dickson concluded that publication of applicants' personal information online violated Saskatchewan's privacy law, asking "[w]hat value is added to the goal of

²³ *Krushell*, at paras. 49 & 50.

²⁴ Investigation Report 2005-001, Office of the Information and Privacy Commissioner of Saskatchewan, January 27, 2005 (online at: <http://www.oipc.sk.ca/Reports/IR2005-001.pdf>).

accountability and transparency by refusing to mask the particular identity of a claimant?”²⁵

A recent finding from the Office of the Privacy Commissioner of Canada dealt with decisions of the Canada Pension Appeals Board and the Office of the Umpire.²⁶ The finding said that decisions published online should be anonymized, by substituting initials for individuals’ names in decisions. The Pension Appeals Board had, according to the complainant, included information such as an individual’s national origin, age, marital status, criminal history, names of children and other information. The complainant said that similar information was available through decisions of the Office of the Umpire. Assistant Privacy Commissioner of Canada Raymond D’Aoust rejected the argument that the open court principle permitted the boards to publish decisions containing personal information on the internet and recommended that they replace names with random initials to protect privacy. He also recommended that the boards apply web robot exclusion protocols²⁷ to the names of individuals identified in past decisions, so that it would not be possible to locate decisions by searching a person’s name on an external search engine.²⁸

Balanced against the privacy considerations illustrated in these decisions, is the significant impact of online access to information to, as the Canadian Judicial Council’s model policy acknowledges, advance the cause of openness:

At the same time, the move towards electronic access raises the possibility that the realization of the open courts principle may be significantly

²⁵ *Ibid.*, at para. 113. The AIAC initially refused to comply with the Commissioner’s recommendation that it de-identify personal information in decisions, but it eventually began using initials, instead of names, making it more difficult to identify the parties involved.

²⁶ The federal agency responsible for handling employment insurance appeals.

²⁷ Robot exclusion protocols enable a webmaster to exclude certain web pages or words from being indexed by search engines such as Google and Yahoo. Other tools, such as XML can be used to facilitate automatic redaction of documents: see Lynn E. Sudbeck, “Placing Court Records Online: Balancing the Public and Private Interests”, *The Justice System Journal*, Vol. 27, Number 3 (2006), at p. 281. While redaction methods are one option, decision-makers should instead follow practices such as those described below, notably exclusion of identifying and unnecessary personal information, as part of the writing process. Creation of multiple versions of a decision with different levels of access and of personal information creates unnecessary risks and complexity.

²⁸ Letter from Raymond D’Aoust, Assistant Privacy Commissioner of Canada, July 8, 2008 (online at: http://www.cippic.ca/uploads/OPCC_ServiceCanada_08Jul2008.pdf).

enhanced. Therefore, restrictions on access should only be justified where the possibility of negative impacts on other values crystallizes into a serious risk. Moreover, any resulting restrictions on access must be carefully tailored in light of their impact on the open courts principle. This is consistent with Canadian constitutional jurisprudence regarding publication bans and other restrictions on the open courts principle.²⁹

With these observations in mind, the following discussion addresses the implications for tribunals of Canadian public sector privacy laws before moving to suggestions for moving forward.

THE PRIVACY FRAMEWORK FOR TRIBUNALS

Unlike the courts, many Canadian administrative tribunals are covered by public sector access to information and privacy protection laws. In Alberta³⁰, Saskatchewan³¹ and Manitoba³², administrative agencies are included in the definitions of “public body”, “government institution” and “government agency.” In Yukon³³ and Nunavut,³⁴ administrative agencies are captured in access and privacy legislation under the definition of “public body”. This is also the case in Newfoundland.³⁵ Federally, administrative agencies are subject to access and privacy legislation because they are included in the definition of “government institution.”³⁶

Ontario’s *Freedom of Information and Protection of Privacy Act*³⁷ covers prescribed agencies, boards, commissions and other bodies; the list of

²⁹ Note 13, above, at para. 20.

³⁰ Freedom of Information and Protection of Privacy Act (online at: http://www.qp.gov.ab.ca/documents/Acts/F25.cfm?frm_isbn=0779729218&type=htm.cfm.)

³¹ *Freedom of Information and Protection of Privacy Act* (online at: <http://www.qp.gov.sk.ca/documents/English/Statutes/Statutes/F22-01.pdf>).

³² *Freedom of Information and Protection of Privacy Act* (online at: <http://web2.gov.mb.ca/laws/statutes/ccsm/f175e.php>).

³³ *Access to Information and Protection of Privacy Act* (http://www.ombudsman.yk.ca/infoprivacy/info_act.html).

³⁴ *Access to Information and Protection of Privacy Act* [S.N.W.T. 1994,c.20] (online at: http://action.attavik.ca/home/justice-gn/attach-en_conlaw_prediv/Type002.pdf.)

³⁵ *Freedom of Information Act* (online at: <http://www.assembly.nl.ca/legislation/sr/statutes/a01-1.htm>).

³⁶ *Privacy Act* (online at: <http://laws.justice.gc.ca/en/P-21/index.html>).

³⁷ *Freedom of Information and Protection of Privacy Act* (online at:

institutions includes the Workplace Safety and Insurance Board and the Ontario Energy Board.³⁸ In British Columbia, the *Freedom of Information and Protection of Privacy Act*³⁹ (“BC FIPPA”) covers administrative agencies and tribunals such as the Securities Commission, Workers' Compensation Board, Human Rights Tribunal and Employment Standards Tribunal.⁴⁰

Canadian access and privacy laws generally exclude communications, notes and draft decisions of decision-makers, essentially to ensure they are not subject to access to information requests. Such laws may apply, however, to final decisions of tribunals. This is not surprising from an access to information perspective, but it does raise the question of the extent to which a tribunal can disclose personal information in its published decisions, online or offline. This arises because bodies covered by privacy laws can only disclose personal information if and to the extent they have the authority to do so under the governing privacy law.⁴¹

Quebec has perhaps the most distinct legislative framework of all for publication of decisions made by tribunals. Quebec access to information law captures administrative bodies,⁴² but, unlike other jurisdictions, the legislation specifically requires public disclosure of tribunal decisions beginning in November 2009. Section 6 of the regulation to Quebec's access and privacy legislation reads as follows:

http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm).

³⁸ R.R.O. 1990, Reg. 460 (online at:

<http://www.canlii.org/on/laws/regu/1990r.460/20080821/whole.html>).

³⁹ Freedom of Information and Protection of Privacy Act (online at:

http://www.qp.gov.bc.ca/statreg/stat/f/96165_01.htm).

⁴⁰ BC's access and privacy law covers many agencies and tribunals, and even covers self-governing professional bodies such as the Law Society of British Columbia and College of Physicians and Surgeons. As discussed below, BC's privacy law does not apply to published decisions of some tribunals.

⁴¹ Similar considerations may arise for labour and commercial arbitrators under Canadian private sector privacy laws. In BC, for example, the *Personal Information Protection Act* does not apply to personal information in notes, communications or draft decisions of decision makers in “administrative proceedings”, whatever those are, but there is no exemption for final decisions. The decisions of arbitrators are not expressly addressed. Nor do the PIPA provisions dealing with non-consensual collection, use and disclosure of personal information clearly address labour arbitration processes and awards.

⁴² *An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information* (online at: <http://www2.publicationsduquebec.gouv.qc.ca/home.php#>).

A public body that makes reasoned decisions in the exercise of adjudicative functions must send the decisions to the Société québécoise d'information juridique, which must distribute them, in accordance with the by-law made under section 21 of the Act respecting the Société québécoise d'information juridique (R.S.Q., c. S-20), through its website on which the decisions of the courts, administrative tribunals and other bodies are published.⁴³

To take British Columbia as another example, BC FIPPA does not apply to notes and draft decisions of a person acting in a “judicial or quasi judicial capacity”,⁴⁴ but final decisions are covered by FIPPA unless the *Administrative Tribunals Act* (“ATA”) applies to the tribunal.⁴⁵ The ATA applies to well known tribunals such as the Workers’ Compensation Appeal Tribunal⁴⁶ and the Human Rights Tribunal,⁴⁷ but it does not cover all tribunals in the province. Moreover, even if the ATA does apply, BC FIPPA is excluded only in relation to a tribunal decision for which public access is provided by the tribunal. Accordingly, where a tribunal covered by the ATA only provides its decisions to the parties, it has to comply with BC FIPPA’s requirements around personal information disclosure.

British Columbia tribunals that are not subject to the ATA can only disclose personal information in their decisions if BC FIPPA allows it. The same is true for disclosure of personal information in decisions of ATA-covered tribunals where the tribunal does not provide public access to decisions. This flows from the fact that tribunals, as public bodies, can only disclose personal information⁴⁸ in

⁴³ *Regulation respecting the distribution of information and the protection of personal information* (online at: <http://www.canlii.org/qc/laws/regu/a-2.1r.0.2/20080818/whole.html>).

⁴⁴ Section 3(1)(b). The reference to action in a “quasi judicial” capacity is archaic and has proved problematic in practice. See *British Columbia (Attorney General) v. British Columbia (Information and Privacy Commissioner) et al.*, 2004 BCSC 1597, [2004] B.C.J. No. 2534 (S.C.).

⁴⁵ Section 61, *Administrative Tribunals Act*, which expressly overrides BC FIPPA and thus ousts its application to tribunal decisions for which public access is provided (online at: http://www.qp.gov.bc.ca/statreg/stat/A/04045_01.htm#section61).

⁴⁶ See *Workers Compensation Act*, s. 245.1 (online at: http://www.qp.gov.bc.ca/statreg/Stat/W/96492_00.htm).

⁴⁷ See *Human Rights Code*, s. 32 (online at: http://www.qp.gov.bc.ca/statreg/Stat/H/96210_01.htm).

⁴⁸ BC FIPPA defines “personal information” as “recorded information about an identifiable individual other than contact information”. The term “contact information” is defined as “information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual”. The concept of what information is about an “identifiable individual” can be vexing. It is touched on below.

accordance with Part 3 of FIPPA. They may disclose personal information for the purpose for which the information was (lawfully) collected—including adjudication of disputes—or for a use that is “consistent” with the purpose for which it was obtained or compiled.⁴⁹ They may also disclose personal information where authorized or required by law,⁵⁰ and governing bodies of professions and occupations may disclose personal information for the purposes of licensing, registration, insurance, investigation or discipline of persons regulated inside or outside Canada.⁵¹ The bottom line is that disclosure of personal information in a particular decision is allowed if it falls under a head of authority under BC FIPPA or a comparable statute.

Even assuming there is statutory authority for a tribunal to disclose personal information in its decisions,⁵² the question arises of the extent to which it should do so. It is well and good to point to legal authority to disclose personal information in published decisions. In view of the well-documented privacy risks relating to internet publication of decisions, outlined above, surely tribunals can and should adopt policies and practices that respect privacy wherever possible, especially in view of the fact that privacy is a right with constitutional dimensions? It bears emphasis that, once personal information is posted online, it is difficult—really, all but impossible—to remove it from the internet. Further, many tribunals deal with vulnerable individuals, who may be ill-equipped to advance their own privacy interests—“[t]hose most likely to be affected by the practice of posting

⁴⁹ Section 34 of BC FIPPA provides that a new use of personal information is consistent with the original purpose for which it was acquired only where (a) the new use has a reasonable and direct connection to the purpose for which it was originally collected and (b) the new use is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses or discloses the information. Ontario’s *Freedom of Information and Protection of Privacy Act* says that a disclosure of personal information is for a consistent purpose if the individual whose personal information is disclosed “might reasonably have expected such a use or disclosure.”

⁵⁰ BC FIPPA, s. 33.1(1)(c).

⁵¹ BC FIPPA, s. 33.1(1)(l).

⁵² At least one expert in this area of the law has concluded that “most agencies are vulnerable because very few can point to statutory direction authorizing let alone compelling the disclosure of personal information in their adjudicative decisions.” See Christopher Berzins, “Personal Information in the Adjudicative Decisions of Administrative Agencies: An Argument for Limits”, *The Advocates’ Quarterly*, July 2008, Vol. 34, No. 3, at p. 283.

adjudicative decisions on agency websites will comprise a diffuse and vulnerable group.”⁵³

Proof that there is a way forward, one that properly balances openness and privacy, is illustrated by the example of what Canadian courts have done in this area.

WHAT THE JUDICIARY HAS DONE

In 2003, the CJC published a discussion paper⁵⁴ about open courts, online access and privacy. In a later summary of the responses⁵⁵ to its paper, the CJC noted “a general consensus that remote public access should be provided to judgments, with privacy concerns dealt with through de-identification protocols for which courts would be responsible”.⁵⁶ The CJC concluded in a 2005 publication that all judgements should be published on the internet to enhance access to justice and facilitate legal research.⁵⁷

The CJC’s model protocol on publication of personal information in court decisions, published in 2005, places the onus on judges, not publishers, to limit disclosure of personal information. It provides specific recommendations for protecting the privacy of personal information, characterized as “omitting personal data identifiers which by their very nature are fundamental to an individual’s right to privacy.”⁵⁸ It identifies certain information, such as name and date of birth, social insurance number and financial account numbers, as being worthy of protection in written decisions because of the risks associated with disclosing them:

⁵³ Berzins, note 46, at p. 279.

⁵⁴ “Open Courts, Electronic Access to Court Records, and Privacy”, Discussion Paper, Canadian Judicial Council (May 2003) (online at: http://www.cjc-ccm.gc.ca/cmslib/general/news_pub_techissues_OpenCourts_20030904_en.pdf.)

⁵⁵ The Canadian Bar Association made a thoughtful submission to the CJC, “Submission on the Discussion Paper: Open Courts, Electronic Access to Court records, and Privacy”, Canadian Bar Association (April 2004) (online at: <http://www.cba.org/CBA/submissions/pdf/04-13-eng.pdf>).

⁵⁶ “Synthesis of the Comments on JTAC’s Discussion Paper on Open Courts, Electronic Access to Court Records, and Privacy” Canadian Judicial Council, at p. 3 (online at http://www.cjc-ccm.gc.ca/cmslib/general/news_pub_techissues_Synthesis_2005_en.pdf.)

⁵⁷ CJC protocol, note 15.

⁵⁸ *Ibid.*, para. 62.

This type of information is susceptible to misuse and, when connected with a person's name, could be used to perpetrate identity theft especially if such information is easily accessible over the internet. Individuals have the right to the privacy of this information and to be protected against identity theft. Except in cases where identification is an issue, there is rarely any reason to include this type of information in a decision. As such, this type of information should generally be omitted from all reasons for judgment. If it is necessary to include a personal data identifier, consideration should be given to removing some of the information to obscure the full identifier.⁵⁹

An appendix to the protocol includes suggestions on removing names from judgements, including a system of using the next letter in a name where two names are identical:

To avoid confusion between many individuals who have the same initials, a fictitious initial is added after the first forename of the other persons named in the decision that have the same initials. This fictitious initial is the second letter of the person's first forename for the second one named, the third letter for the third named, and so on.

Examples

<u>Names</u>	<u>Replaced by</u>
John McKeown and James Morgan	J.M. and J.A.M.
Mary Jane Davis and Mark John	M.J.D. and M.A.J.D. Dalton
Mary, Mark and Mario Davis	M.D., M.A.D. and M.R.D. ⁶⁰

The CJC also produced a model policy document for access to court records. It echoes the protocol recommendations by placing the onus on judges and court staff, not publishers, to make efforts to protect personal information:

⁵⁹ *Ibid.*, para. 23.

⁶⁰ "Use of Personal Information in Judgments and Recommended Protocol" at para. 40 (online at: http://www.cjc-ccm.gc.ca/cmslib/general/news_pub_techissues_UseProtocol_2005_en.pdf).

When judges and judicial officers draft their judgments and, more generally, when court staff prepare documents intended to be part of the case file, they are responsible for avoiding the disclosure of personal data identifiers and limiting the disclosure of personal information to what is necessary and relevant for the purposes of the document.⁶¹

THE WAY FORWARD—WHAT TRIBUNALS CAN DO

Although an open court is the rule rather than the exception, the CJC's publications have clearly underscored the need to protect personal information in judgements in an era when paper filing in central locations has given way to judgements that are indexed and searchable from anywhere in the world. This does not challenge the open court principle, it refines it. The case for action is acknowledged in a recent British Columbia government discussion paper,⁶² yet, as an Alberta government policy paper has recently observed, there is little uniformity in the practice of administrative tribunals in Canada.⁶³ There are, however, steps that tribunals can, and should take, some of which are discussed below.

Most administrative tribunals in Canada are subject to access and privacy legislation that places restrictions on disclosing personal information. Unlike tribunals, the courts are generally specifically excluded from access and privacy legislation, but they are subject to the open court principle. Despite having no statutory or common law restrictions on the kind of personal information they can disclose, however, the courts have recognized the need to protect personal information in an era of unprecedented public access to decisions via the internet.

⁶¹ "Model Policy for Access to Court Records in Canada", *Canadian Judicial Council* at pg. 18 (online at:

http://www.cjc-ccm.gc.ca/cmslib/general/news_pub_techissues_AccessPolicy_2005_en.pdf).

⁶² "Statutory Decision-Makers and the Obligation to Give Reasons for Decisions", Administrative Justice Office, Ministry of Attorney General, British Columbia (September 2008) (online at: http://www.gov.bc.ca/ajo/down/reasons_paper092008.pdf).

⁶³ "Disclosure of Personal Information in Decisions of Administrative Tribunals", Alberta Government Services (July 2002). The paper also acknowledged that, in many circumstances, tribunals post decisions online even where their governing legislation does not necessarily expressly deal with making their reasons for decision publicly available.

To address privacy considerations, an administrative tribunal's reasons for decision should exclude personal information unless the reasons would not be adequate without that information. After drafting their reasons, decision makers should evaluate, as part of the process of revision and editing, whether individuals are identifiable and whether the information that identifies them is necessary for explaining the reasons for a decision. Properly implemented, this approach will protect privacy of parties and witnesses while preserving intelligibility and adhering to the principle of openness.

Administrative tribunals should follow the courts and ensure that they do not include unnecessary personal identifiers in decisions. Suggestions to protect privacy include:

- providing notice to parties (and witnesses where feasible) that decisions will be made available online;
- replacing names of parties and witnesses with initials (or, where feasible, general terms like “applicant”, “complainant”, “respondent”);⁶⁴
- not including a party's date of birth or age;
- not including an individual's workplace or residential address;
- not including a party's place of residence if they are from a small town⁶⁵;
- not including information such as bank details, driver's licence numbers or social insurance numbers;
- not including information about an individual's marital status, sexual orientation, national origin, criminal history, medical history unless it is truly necessary to do so;
- for internet publication, using robot exclusion protocols where names cannot be removed, so that names will not be indexed by search engines outside the tribunal's website;⁶⁶

⁶⁴ See the CJC protocol's suggestions, discussed earlier in this paper.

⁶⁵ In addition, it may be helpful to omit any unique information or other unusual identifiers that could allow a reader to determine who a party is even if their name has been removed.

⁶⁶ Berzins, note 45, at p. 283.

-
- if decisions of a tribunal are posted on that tribunal's website, consider excluding a field that allows users to search by party name.⁶⁷

In pursuing such measures, tribunals should remember that the practical obscurity of paper is all but gone. Scanning technology enables anyone to scan and post a paper document online in minutes. This means that decision makers should determine whether personal information needs to be included in all decisions, even paper versions not intended for online posting in electronic form by the tribunal itself.

CONCLUSION

This paper provides only a high-level review of some of the challenges tribunals face in their efforts to fulfill the policy objectives of the open court principle while protecting personal information appropriately. No one suggests that privacy should defeat the vital principles of openness and accountability in tribunal processes. That said, where individuals are caught up in tribunal processes, their privacy deserves respect and protection. This is not a zero sum game. Tribunals can follow the lead of Canada's judiciary in protecting privacy while discharging their duties in as open a fashion as possible.

* * *

⁶⁷ See Elizabeth Judge, "Canada's Courts Online: Privacy, Public Access and Electronic Court Records", in *Dialogues About Justice: The Public Legislators, Courts and the Media/ Dialogues Sur La Justice: Le Public, Le Legislatateur, Les Tribunaux et Les Médias*, Patrick A. Molinari, ed., Canadian Institute for the Administration of Justice (Montreal: Les Editions Thémis, 2002), 1-26, at p. 24 (online at: http://www.ciaj-icaj.ca/francais/publications/2002/JudgeElisab_1-26.pdf).