Model Policy for Access to Court Records in Canada

Judges Technology Advisory Committee

Canadian Judicial Council

September 2005

Executive Summary

In May 2003, the Canadian Judicial Council released a discussion paper prepared by the Judges Technology Advisory Committee (JTAC) entitled "Open Courts, Electronic Access to Court Records, and Privacy," which built upon an earlier report for the Administration of Justice Committee of the Council. This discussion paper assembled 33 conclusions including that the right of the public to open courts is an important constitutional rule, that the right of an individual to privacy is a fundamental value, and that the right to open courts generally outweighs the right to privacy. The discussion paper also concluded that the Canadian Judicial Council has a leadership role in initiating discussions and debate about the development of electronic access policies and that such policies be as consistent as possible throughout Canada. The Council then invited public comment on the many policy and logistical issues that were developed within the discussion paper so that it could move towards framing a model policy on electronic access.

The results of the public consultation regarding the discussion paper are available in the report prepared for JTAC entitled "Synthesis of the Comments on JTAC's Discussion Paper on Open Courts, Electronic Access to Court Records, and Privacy." This report summarizes the many responses received by JTAC, indicates where there is an emerging consensus on the issues, and develops a principled framework for the development of a model policy on access to court records. Such a policy must acknowledge two possibilities that arise from the move towards electronic access. The first is that the realization of the open courts principle may be significantly enhanced through the adoption of new information technologies. The second is the possibility that unrestricted electronic access might facilitate some uses of information that are not strongly connected to the underlying rationale for open courts and which might have a significant negative impact on values such as privacy, security, and the administration of justice. Given this, the proposed guiding principles for an access policy are:

(a) The open courts principle is a fundamental constitutional principle and should be enabled through the use of new information technologies.
(b) Restrictions on access to court records can only be justified where:

i. Such restrictions are needed to address serious risks to individual privacy and security rights, or other important interests such as the proper administration of justice;
ii. Such restrictions are carefully tailored so that the impact on the open courts principle is as minimal as possible; and
iii. The benefits of the restrictions outweigh their negative effects on the open courts principle, taking into account the availability of this information through other means, the desirability of facilitating access for purposes strongly connected to the open courts principle, and the need to avoid facilitating access for purposes that are not connected to the open courts principle.

As a result of this preliminary work, as well as further research, the Canadian Judicial Council proposes the following "Model Policy for Access to Court Records in Canada." Although there might be a number of different ways in which to draft a policy that is consistent with these guiding principles, the model proposed is the one that the Canadian Judicial Council considers to be the most consistent with the emerging national consensus on these questions, acknowledging that there remain a number of elements on which there is some disagreement. The Canadian Judicial Council hopes that this model policy can serve as a basis for the development of access policies in the courts of Canada. At the very least it is hoped that this model policy can serve to foster further national discussion on these issues.

In summary, this policy endorses the principle of openness and retains the existing presumption that all court records are available to the public at the courthouse. When technically feasible, the public is also entitled to remote access to judgments and most docket information. This policy does not endorse remote public access to all other court records, although individual courts may decide to provide remote public access to some categories of documents where the risks of misuse are low. In addition, users may enter into an access agreement with the court in order to get remote access to court records, including bulk access. Finally, this policy develops many of the further elements of an access policy, including provisions relating to the creation, storage and destruction of court records.

Table of contents

Introduction

Background

[1] The Judges Technology Advisory Committee (JTAC) is an advisory committee of the Canadian Judicial Council (the Council). The mandate given to JTAC by the Council includes the following:

- Providing advice and making recommendations to the Council on matters relating to the effective use of technology by the courts, consistent with the Council's overall mandate to promote uniformity and efficiency and improve the quality of judicial service in courts across the country;
- Supporting the development of standards for judicial information, court filings, evidence, judgments and other information in electronic form;
- Monitoring and considering technical issues that may have an impact on access to justice.

[2] In March 2002, Chief Justice of the Supreme Court of British Columbia, Donald I. Brenner and his Law Officer, Judith Hoffman prepared a report for the Administration of Justice Committee of the Council, entitled "Electronic Filing, Access to Court Records and Privacy". In the report, the authors identified and considered some of the policy and logistical issues arising from electronic filing and electronic access to court records. The Administration of Justice Committee received that report and referred it to JTAC. In response, in April 2002, JTAC created a subcommittee which included Chief Justice Brenner (Supreme Court of British Columbia), Judith Hoffman (Law Officer, Supreme Court of British Columbia), Jennifer Jordan (Registrar, Court of Appeal of British Columbia), Justice Frances Kiteley (Superior Court of Ontario), Justice Denis Pelletier (Federal Court of Appeal) and Justice Linda Webber (Supreme Court of Prince Edward Island, Appeal Division). JTAC directed the subcommittee to make proposals for its consideration.

[3] Building upon the work of the initial report for the Administration of Justice Committee of the Council, the JTAC subcommittee prepared a discussion paper entitled "Open Courts, Electronic Access to Court Records, and Privacy" (the Discussion Paper). Reviewing the jurisprudence of the Supreme Court of Canada, the Discussion Paper generated 33 conclusions on various issues connected with the constitutional right of the public to open courts, the right of individuals to privacy and many of the policy and logistical issues pertaining to access to court records if electronic and remote access is granted to the public. This paper was considered by JTAC at its meeting in May, 2003 and released for public comment in September 2003 (online at <http://www.cjc-ccm.gc.ca>).

[4] Up until April 2004, the Council received many responses to its Discussion Paper from Deputy Attorneys General, judges, other members of the legal profession,

academics and representatives of the media. The Council directed JTAC to prepare a synthesis of the responses and to draft a model policy on access to court information.

[5] JTAC engaged Lisa Austin, Assistant Professor at the University of Toronto Faculty of Law, and Frédéric Pelletier, Assistant Editor at CanLII and Research Officer at the University of Montreal's Centre de recherche en droit public, to synthesize these responses and, under the direction of the subcommittee, to draft this model policy on access to court records. The subcommittee and JTAC are grateful for the enormous contribution that Professor Austin and Mr. Pelletier have made to this evolving and challenging exercise. Without their expertise, this project could not have been accomplished.

The Issues at Stake

[6] Canadian courts have consistently held that the openness of court proceedings is an important constitutional principle that fosters many fundamental values, including public confidence in the judicial system, understanding of the administration of justice, and judicial accountability. Included within the open courts principle is the public's right of access to court records.

[7] Traditionally, court records have been accessible in paper format to any member of the public at the courthouse. There are some exceptions to this, namely for records that are sealed by a court order or pursuant to a statutory requirement. However, in general any person who can afford a trip to the court registry may ask a court clerk to see all documents and information pertaining to a specific case.

[8] This traditional way of obtaining access to court records is becoming more and more obsolete. Courts still store their court files in paper format, but most docket or case information is now kept in electronic databases in which a user may find information much more easily than in the former paper ledgers. Several courts are also adopting electronic filing, which potentially increases the availability of records since the information and actual documents in the court file may be stored in digital formats. Moreover, access to recent court decisions has never been better since many courts make them publicly available on the internet at no charge. The overwhelming trend, therefore, is for courts to adopt digital formats for court records in order to make preparation, storage and access to court information easier and more efficient.

[9] In addition to this trend towards the adoption of court records in digital format is the increasing availability of electronic networks such as the internet that could be used to obtain remote and bulk access to court information along with the use of powerful search tools. Through these new technologies it will become possible to retrieve more information about court proceedings and their participants than ever before, not only in terms of quantity, but also in terms of quality since such information can be aggregated or combined with other publicly available information. The resulting ability to break down the practical barriers to access to court records has the potential to greatly enhance the realization of the open courts principle for all members of the public.

[10] However, there are also potential drawbacks to the adoption of new technologies in relation to court records: new technologies increase the risks that court information might be used for improper purposes such as commercial data mining, identity theft, stalking, harassment and discrimination. Such uses can undermine the proper administration of justice and threaten the rights and interests of participants in judicial proceedings, including their privacy and security interests. In many ways, the "practical obscurity" of paper-based records, because it created a barrier to access, also provided de facto protection for some of these other values such as privacy. Now that barriers to access may be dramatically reduced, the question of whether and how to protect such values in the context of access to court records has become much more salient.

[11] As the Canadian Judicial Council's Discussion Paper outlined, "[a]t the heart of the matter is the relationship between two fundamental values: the right of the public to transparency in the administration of justice and the right of an individual to privacy." After surveying the existing jurisprudence regarding the open courts principle, the Discussion Paper concluded:

- the right of the public to open courts is an important constitutional rule;
- the right of an individual to privacy is a fundamental value; and
- the right to open courts generally outweighs the right to privacy.

However, the Discussion Paper also acknowledged that "[t]here is disagreement about the nature of the exemptions to the general rule." The challenge for courts is to construct a policy for access to court records that can maximize the many benefits of new information technologies with respect to the realization of the open courts principle while determining what kinds of exemptions are warranted.

[12] Drawing upon the responses to the Discussion Paper, this model policy outlines a set of guiding principles with respect to the relationship between the open courts principle and other important constitutional values such as privacy. In addition, it is important to note that just as new information technologies can raise new issues with respect to access to court records, such technologies can also offer new solutions. In the past, exemptions to the general rule of openness have led to the use of such judicial tools as publication bans and sealing orders. New technologies offer the possibility of many more nuanced responses that can protect values such as privacy without the same dramatic impact on openness. Therefore, in addition to articulating a principled framework for treating the question of exemptions to the principle of openness, this model policy also addresses many of the more technical aspects of the careful tailoring called for by any exemptions to openness.

Responses to the Discussion Paper

[13] The Council received many responses to its Discussion Paper, which are documented in more detail in the report entitled, "Synthesis of the Comments on JTAC's Discussion Paper on Open Courts, Electronic Access to Court Records, and Privacy." Although these responses were not unanimous with respect to the issues raised by electronic access to court information, there were some significant points of agreement.

[14] First, there was strong agreement with respect to the central importance of the open courts principle, as well as the Discussion Paper's conclusion that "[t]he right to open courts generally outweighs the right to privacy."

[15] Second, there was also strong agreement with respect to the potential problems associated with permitting unrestricted electronic access to court records. For example, there were concerns regarding bulk searches of court records in electronic form, especially if commercial entities could engage in forms of data-mining. A number of other privacy and security concerns were consistently raised, including identity theft and the possibility of the harassment of participants in the judicial system.

[16] While there was more variability in the comments dealing with the desirability and feasibility of the types of restrictions on access which might be used to address privacy and security considerations, nonetheless there were areas of broad agreement:

a) There was a general consensus that remote access to the contents of all court records is not desirable for the public. Suggestions to deal with privacy concerns with court records include implementing de-identification protocols, indicating that a document exists without providing details regarding its contents, providing differing levels of access to different categories of users, and exempting "sensitive" records from remote access entirely;
b) There was a general consensus that members of the public should not have the right to run unrestricted bulk searches;
c) There was a general consensus that remote public access should be provided to reasons for decision, with privacy concerns dealt with through de-identification protocols for which courts would be responsible;
d) There were mixed views regarding remote public access to docket information, partly because of the inconsistent cross-jurisdictional approaches to what is included within docket information. Suggestions to deal with privacy concerns with docket information included implementing de-identification protocols, charging fees for remote access, providing remote access only to specific categories of users, or restricting remote access entirely.

Guiding Principles

[17] The following model policy seeks to reflect the consensus that emerged from the responses to the Discussion Paper and place that consensus within a principled framework. Such a framework must offer a way of addressing the relationship between the open courts principle and other important values such as individual privacy, security, the proper administration of justice as well as the timely conduct of judicial proceedings.

[18] As already indicated, new information technologies have the potential to significantly enhance access to court records. At the same time, such technologies threaten to undermine the "practical obscurity" of traditional paper-based records which has provided a kind of de facto protection for values such as privacy and security. A focus on the benefits of broad access would emphasize the need for unrestricted online access to court record information. A focus on the protections of "practical obscurity" would emphasize the need to reproduce such protections in the online environment. This

model policy outlines a third option by proposing a different way of thinking about the significance of "practical obscurity" and its relation to the open courts principle.

[19] 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.

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

[21] The model policy is therefore built upon the following principled framework:

(a) the open courts principle is a fundamental constitutional principle and should be enabled through the use of new information technologies;

(b) restrictions on access to court records can only be justified where:

i. such restrictions are needed to address serious risks to individual privacy and security rights, or other important interests such as the proper administration of justice;

ii. such restrictions are carefully tailored so that the impact on the open courts principle is as minimal as possible; and

iii. the benefits of the restrictions outweigh their negative effects on the open courts principle, taking into account the availability of this information through other means, the desirability of facilitating access for purposes strongly connected to the open courts principle, and the need to avoid facilitating access for purposes that are not connected to the open courts principle.

Purpose of this Model Policy

[22] The purpose of the Council in developing this model policy is not to state legal rules governing access to court records. Its purpose is rather to provide courts with a framework to deal with new concerns and sensitive issues raised by the availability of new information technologies that allow for unprecedented access to court information. This model policy was designed to help Canadian courts develop their own policies of access to their records, thus assuming their supervisory and protective power over these records, in a manner that is consistent with the consensus that is emerging in Canada and in other countries on these issues, including the recent Canadian Judicial Council report,

"Use of Personal Information in Judgments and Recommended Protocol" (online: <http://www.cjc-ccm.gc.ca/article.asp?id=2811>). This model policy is also consistent with the current constitutional framework that applies in Canada with regard to the balance that needs to be struck between the open courts principle and other important values, such as privacy, security and the administration of justice.

[23] The Canadian Judicial Council hopes that this model policy can serve as a basis for the development of access policies in the courts of Canada. Access policies developed with the help of this model policy will be used by the judiciary as guidelines for drafting and revising several aspects of their internal rules of practice and other court rules that have an impact on issues related to access to court records.

[24] Despite the efforts made by the Council to gather and reconcile various viewpoints, this model policy may contain several elements upon which some disagreement will remain. The risks to personal privacy rights must be assessed in specific social and technological contexts, taking into account not only real threats, but also perceived threats that have an impact on the behavior of participants in judicial proceedings. These risks can be managed only in a specific context. Furthermore, the technological solutions that might prevent or circumvent many of these risks are not yet fully realized. Time and experience will certainly allow for a better assessment of the risks, and as new technology is implemented in courts to manage their information, many issues will be better addressed. In the mean time, courts that are implementing this model policy are invited to share their experiences and solutions with the Council, so that the Council may continue to foster a national discussion on these issues.

Model Policy for Access to Court Records in Canada

1 General Provisions

1.1 Purpose

The purpose of this policy is to define principles of access to court records, consistent with applicable statutory and common law rules, so as to guide the judiciary in the exercise of its supervisory and protective power over court records. The principles stated in this policy are the result of a balancing of the constitutional requirement of open courts against other rights and interests of the public and participants to judicial proceedings, namely privacy and security of individuals and the proper administration of justice.

Discussion

Openness of court proceedings is a fundamental constitutional principle that ensures public confidence in the integrity of the court system, better understanding of the administration of justice and accountability of the judiciary. The open courts principle not only ensures that members of the public have a right to attend proceedings in the courtroom, but also that all information that is part of the court record and that is not confidential according to statutes or common law must remain open to public scrutiny.

Any access policy developed by the judiciary on the basis of this model policy will be founded upon the inherent jurisdiction of the judiciary to maintain supervisory and protective power over its own records. Thus, it must be clear that any reference made in this model policy to the "court" does not include the administrative aspects of the court for which the executive branch of the government is responsible, but only the judiciary in the exercise of a judicial function such as its supervisory and protective powers regarding court records.

Openness is the core principle upon which any policy for access to court records should be developed. At the same time, a policy must aim at addressing other important but sometimes competing rights and interests, such as privacy and security of individuals and the proper administration of justice. These two elements summarize many concerns and issues that are most often raised in regard to open access to court records, namely, public safety, protection of confidential business information, efficacy of court administration, timely conduct of court proceedings, etc.

In the context of the emergence of new information technologies, many benefits are expected with regard to open access to court records. At the same time, unrestricted access to court records also carries with it potential encroachments on individual privacy and security rights. In particular, new means of access to records pose new threats to those rights, such as data mining, identity theft, stalking, harassment and discrimination. Moreover, if court records are accessed and utilized for improper purposes or in a manner that subverts justice, then public confidence in the administration of justice might be undermined. Various statutory provisions and common law measures, including such mechanisms as sealing orders and publication bans, are already available to protect

these interests. However, these are blunt tools that have a significant impact on the open courts principle. New technologies and methods can provide other options for protecting such interests in a manner that permits much more careful tailoring of restrictions on access, including segregating some kinds of sensitive data in records and utilizing drafting protocols that minimize the insertion of personal data in the court record.

A careful analysis of each of these issues in a given context is key to determining how access will actually be provided to the public and how any restriction to such access could be narrowly tailored so as to fully achieve open access while minimizing the risks that this information is used for improper purposes.

1.2 Scope and Application

1.2.1 Persons Covered

This policy sets out the principles governing the public's access to court records. It is not intended to apply to the availability of court records to the judiciary and court personnel.

Discussion

This model policy does not apply to judges and other court personnel and is not intended to interfere with the applicable internal rules and practices of the court regarding the daily business of the court's judiciary and court personnel.

1.2.2 Type of Proceeding

This policy applies to court records in both civil and criminal proceedings, at both trial and appeal levels, unless otherwise indicated.

Discussion

Distinctions may need to be made depending upon the type of proceeding, e.g. family, criminal or youth protection proceedings. There might also be distinctions to make between trial and appeal levels of court. This model policy does not make these distinctions but nevertheless presents various levels of access that could be adopted for various types of records.

1.2.3 Form of Court Record

This policy covers all court records in any form, whether these records are created, stored or made available on paper or in digital format.

Discussion

This model policy contains guiding principles that are, whenever possible, framed in a manner that is technologically neutral. Although most Canadian courts are moving towards maintaining records in electronic format, the technologies implemented to manage electronic records can differ across different court systems. Furthermore, this

model policy should be adaptable to the possibilities of emerging technologies. Because of this, the rights of access outlined in this model policy are not premised upon the particular format of court records (paper vs. electronic) but instead are expressed in terms of functionality, that is, in terms of what level of access should result from the processes and mechanisms that are put in place to ensure such access to different types of court records.

Of course, for the sake of clarity, an access policy may specify the form in which a record can be accessed in accordance with a specific technological environment. For example, when a court allows any member of the public to search in its electronic docket information system at the courthouse, it is much clearer to refer to this specific system in its electronic form. The specific name of the system may also be used, e.g. "JUSTIN" in British Columbia or the "Plumitifs" in Quebec.

1.2.4 Other Applicable Laws

The access provided for in this policy is subject to any applicable statutory or common law provision regarding access to, or publication of, court records.

Discussion

For more clarity and better consistency, courts may add, as an appendix to their policy, a compendium of applicable statutory and common law restrictions that might be of particular importance in their jurisdiction with regard to rights of access to court records. It should be noted that court records are exempt from provincial and federal access to information legislation.

1.3 Definitions

1.3.1 Access

"Access" means the ability to view and to obtain a copy of a court record.

Discussion

This definition of access includes the ability to obtain a copy of a court record since such a copy might be necessary for the efficient exercise of the public's right of access. In some jurisdictions, however, the current statutes and rules of access provide only for the right to see the document, remaining silent about the issue of obtaining copies of documents.

Courts that offer electronic access should also examine compliance to accessibility standards for the physically impaired in the virtual world. For documents posted on websites, for instance, courts may want to make their web pages compliant to the W3C's Web Content Accessibility Guidelines (online: <http://www.w3.org/TR/WCAG10/wai-pageauth.html>).

1.3.2 Case File

"Case file" refers to docket information and documents in connection with a single judicial proceeding, such as pleadings, indictments, exhibits, warrants and judgments.

1.3.3 Court Records

"Court records" include any information or document that is collected, received, stored, maintained or archived by a court in connection with its judicial proceedings. It includes, but is not limited to:

a) **case files;**
b) **dockets;**
c) **minute books;**
d) **calendars of hearings;**
e) **case indexes;**
f) **registers of actions; and**
g) **records of the proceedings in any form.**

This definition does not include other records that might be maintained by court staff, but that are not connected with court proceedings, such as license and public land records. It does not include any information that merely pertains to management and administration of the court, such as judicial training programs, scheduling of judges and trials and statistics of judicial activity. Neither does it include any personal note, memorandum, draft and similar document or information that is prepared and used by judges, court officials and other court personnel.

1.3.4 Docket

"Docket" means a data system in which court staff collect and store information about each proceeding initiated before the court, such as:

a) **information about the court division and type of case;**
b) **docket number;**
c) **names and roles of parties;**
d) **names of counsel or solicitors of record;**
e) **names of judges and judicial officers;**
f) **nature of proceedings, including cause of action or criminal informations and indictments;**
g) **information about the requested relief or amount of damages;**
h) **list and corresponding filing dates of documents present in the case file;**
i) **dates of hearings; and**
j) **dispositions with their corresponding dates.**

Discussion

The definitions of case file, court record and docket may vary from one jurisdiction to another. In this model policy, these three definitions play an important role in the recommended rights of access to different types of information contained in the court record. However, their content and wording should be adapted to the types of records in a specific court or jurisdiction.

The definition of "case file", in this model policy, is premised on the assumption that the parties should have unrestricted access to records that pertain to their own case. Docket information relating to a single case is also considered to be part of the case file.

The definition of "court record" sets out what elements of information fall within the scope of an access policy to court records, and which elements do not. This information is presumptively open for public access according to this model policy.

The definition of "docket" identifies all the basic elements of information relating to cases managed by a court. The content and availability of docket information varies from one jurisdiction to another, so special care should be brought to adapt the terms used in this definition. Applicable statutes and rules of court may also dictate some adaptations.

1.3.5 Judgment

"Judgment" refers to any decision rendered by judges or judicial officers, including endorsements and orders, as well as any disposition or reasons given in connection with such decision.

Discussion

This definition may include oral reasons, depending upon whether or not the court administration makes them available in audio or written form.

1.3.6 Parties

"Parties" include the parties, their counsel and other authorized agents.

1.3.7 Personal data identifiers

"Personal data identifiers" refers to personal information that, when combined together or with the name of an individual, enables the direct identification of this individual so as to pose a serious threat to this individual's personal security. This information includes:

a) day and month of birth;
b) addresses (e.g. civic, postal or e-mail);
c) unique numbers (e.g. phone, social insurance, financial accounts); and
d) biometrical information (e.g. fingerprints, facial image).

"Personal data identifiers" does not include a person's name.

Discussion

Personal data identifiers are the subset of personal information that is the most important and valuable for any individual, since they are used by institutions to authenticate a person's identity, apart from an individual's name. Personal data identifiers also typically allow direct contact with an individual. Unrestricted public access to this type of personal information would entail serious threats to personal security, such as identity theft, stalking and harassment, and the foreseeable uses of this information are not likely to be connected with the purposes for which court records are made public.

It must be noted that this definition of "personal data identifiers" does not include the name of an individual per se, since the risks stated above usually occur when these elements of information are combined with an individual's name.

This model policy will refer to personal data identifiers as information that should not be widely accessible to the public. Even if the names of individuals in court proceedings remain public, there is no rationale for making their personal data identifiers widely available.

This use of "personal data identifiers" is consistent with the Canadian Judicial Council's "Use of Personal Information in Judgments and Recommended Protocol" (online: <http://www.cjc-ccm.gc.ca/article.asp?id=2811>).

1.3.8 Personal Information

"Personal information" is information about an identifiable individual.

Discussion

This definition conforms to the common meanings of this term. Information about an identifiable individual singles out a person as a unique individual, allows for this person's identification or allows someone to learn something about this person. Depending upon the context, certain personal information is considered private and other personal information is considered public.

In the judicial context, the level of personal information that is considered public is a function of what information is required for the disposition of a case, subject to any applicable disclosure restrictions. Unless a record is sealed or is the subject of a publication ban, individuals are usually not protected from being named in judicial proceedings. Their other personal information is not usually protected either. However, since every individual has at least some interest in protecting his or her personal information, an access policy to court records should limit the level of personal information found in court records to that required for the disposition of a case.

1.3.9 Registered Access

"Registered Access" is a means of access that entails identification of the person who is granted certain rights of access. This means of access may also involve the logging of requests made by this person during a session.

Discussion

Registered access is a technical means of granting various levels of access to identified persons, in accordance with the access policy. The person must provide identification, either as an individual or as a member of an organization, with a user identification code and a password. Registered access may also be used to keep track of this person's activities during a logged session. The log may contain a record of every request that was made and of each piece of information that was consulted. This is useful to check for unlawful or abusive uses of an individual's rights of access. Of course, user tracking should be governed by a strict privacy policy, of which the user should be made aware. This privacy policy should minimally guarantee that only necessary information will be collected, that the log will be kept confidential, that it will be consulted by a limited number of authorized court staff, and only if needed for the purpose of verifying whether the user is breaching the terms and conditions of access or is performing other unlawful or abusive activities (See the federal Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, which provides, in its Schedule 1, principles that should underlie any such privacy policy).*

This model policy uses registered access as a potential condition in special access agreements to ensure that where access is granted on certain conditions that it is used in compliance with those conditions. For example, since parties are given full remote access to their case files but the public is not, it is important to be able to identify the user. Registered access will also typically be included as conditions of use when extended access is granted to certain persons pursuant to Section 5, below, e.g. bulk or remote access to all case files or a subset of case files.

1.3.10 Remote Access

"Remote access" means the ability to access court records without having to be physically present where the records are kept, and without needing the assistance of court personnel.

Discussion

This definition describes what usually constitutes remote access to an electronic repository of information, available through the internet or any other distant connection. This type of access is more likely to represent privacy and security risks since the court relies on technology to provide access and there is no court staff to filter each access request.

In this model policy, this type of access will typically require special safeguards and may be governed by terms and conditions included in an access agreement.

Certain courts may want to include traditional means of remote access in their access policy, such as when it is possible for a person to call a court clerk by phone to request that a copy of a court record be prepared and sent by mail. In this model policy, this type of access is treated like any access at the courthouse, since it poses the same very low level of risk.

For more clarity, a reference could be made in this definition to the specific systems that fulfill the functionality that is described in this definition, e.g. an electronic docket system available through a court's website.

2 Creation

2.1 Inclusion of Personal Information

Rules that govern the filing of documents in the court record shall prohibit the inclusion of unnecessary personal data identifiers and other personal information in the court record. Such information shall be included only when required for the disposition of the case and, when possible, only at the moment this information needs to be part of the court record.

2.2 Responsibilities of the Parties

When the parties prepare pleadings, indictments and other documents that are intended to be part of the case file, they are responsible for limiting the disclosure of personal data identifiers and other personal information to what is necessary for the disposition of the case.

2.3 Responsibilities of the Judiciary

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.

Discussion

The access policy must prevent the inclusion of unnecessary personal data identifiers and other personal information when the court record is created in order to reduce the amount of personal information that will have to be stored and potentially made accessible to the public. The policy must also clearly outline the responsibilities of those who prepare documents that will be included in the court record.

With regard to the disclosure of "personal data identifiers" as defined in this model policy, the requirements for pleadings prepared by the parties are less strict than those for documents prepared by the court. There are two major reasons for this. First, personal data identifiers are less likely to be relevant for the purposes of the judgments than they are for the filing requirements of pleadings or indictments. Second, unlike documents filed by the parties, judgments are much more likely to be published in case law reports and databases, so the inclusion of personal data identifiers in these documents would constitute a much higher risk for the personal safety of participants in judicial proceedings.

The onus of limiting personal information in the court record rests on the persons who draft or prepare documents that are intended to be part of this record, as these persons are in the best position to be aware of the presence of such information. Judges drafting judgments should follow the above-mentioned document from the Canadian Judicial Council entitled "Use of Personal Information in Judgments and Recommended Protocol" (online: <http://www.cjc-ccm.gc.ca/article.asp?id=2811>).

The implementation of this section may require a reexamination of the statutes and rules of practice. Prescribed forms may have to be revisited, as well as case workflow processes. For instance, while the documents would continue to be served on other parties, filing requirements for documents which contain sensitive personal information should permit the filing of such documents at the latest practicable date before their use is required in the proceedings.

3 Storage

When storing court records, the court should ensure, where possible, that personal data identifiers and other personal information that should not be disclosed to the public are capable of being segregated from other documents or information found in the court record.

Discussion

The access policy should provide for easier management of personal data identifiers and other personal information that must be collected and stored in the court file. Because of the risks that are triggered by the disclosure of personal data identifiers (e.g. identity theft, harassment, stalking), the manner in which the court stores this information becomes key for ensuring that the security rights of litigants are protected when their case information is accessed by third parties.

Docket information is now usually stored in an electronic database that allows for the efficient management of information about a case and for different levels of permission for access. In this way, public access to certain information – especially personal data identifiers – can be restricted for certain types of cases without completely restricting public access to other docket information. This should be brought to the attention of the court administration when choosing and implementing a case management technology.

When court administrations do not have the resources and technical means to implement such segregation of personal information, remote access to certain information or documents should be restricted. For example, if identities of participants in child protection proceedings should not be published and the court does not have the means to store their names as a specific hidden field in their docket, then docket information pertaining to this type of proceeding should not be made publicly available on this court's website for members of the public.

4 Access

4.1 Presumption of Access

Members of the public have presumptive right of access to all court records.

Discussion

The access policy should clearly state the principle of public access to court records. It is placed first in this section in order to emphasize the importance of the open courts principle.

4.2 Fees

Fees should not impede access under this policy.

Discussion

Tailored access to court information, remotely and in electronic format, might require the acquisition and operation of advanced information management systems, and in some jurisdictions the implementation of such systems might not be possible without asking users to contribute. However, case management systems may also reduce court administration costs, and overall may result in global savings. Those savings should serve the purpose of open courts and contribute to the reduction of access fees. The court should at the very least make sure that traditional access on the court premises will remain possible at no extra cost for members of the public.

4.3 Existence of a Case File

Members of the public are entitled to know that a case file exists, even when a case file is sealed or subject to a non-publication order.

Discussion

Public knowledge of the existence of a case file is a minimal requirement for openness, this being all the more important when the file is sealed. In such cases, the disclosure of the existence of a case file should be made in a manner that does not disclose its content. However, it must be stated that as provided for in Section 1.2.4 of this model policy, this section is subject to any applicable statutory provision prohibiting the disclosure of the existence of a file, such as any applicable provision related to national security.

4.4 Format of Records

Members of the public are entitled to access court records in the format in which they are maintained.

Discussion

This model policy allows for a progressive transition from traditional forms of access to more advanced technologies, namely from paper records to digital documents. However, each court may want to state more specifically which formats of access are actually provided to the public, e.g. paper, electronic, or both.

4.5 Search Functions

When accessing court records, members of the public shall be provided with appropriate search functions that allow for efficient research of court records but also limit the risk of improper use of personal information.

Discussion

Search functions should be made available to users who have access to court records. The availability of search tools should depend upon the type of court record accessed and the level of risk of misuse of information associated with the means of access provided.

Search tools can be designed in a manner that limits the technical possibility of aggregation of information and secondary uses that are not related to the rationale for open access to court records, such as direct marketing solicitations. Such limitations include allowing searches only in certain fields of information and not allowing full text searches.

Section 4.6, below, contains specific recommendations as to what search functions should be made available to the public with regard to specific types of records and means of access.

4.6 Type of Record and Means of Access

4.6.1 Judgments

Members of the public shall have on-site access and, where available, remote access to all judgments.

Discussion

The access policy should provide for broad public access to every judgment rendered by the court, subject to any applicable statutory or court-ordered publication ban.

Online publication of judgments containing personal information about vulnerable persons involved in certain categories of cases, such as children and adults in need of protection, is a controversial issue. The evaluation of the level of risk associated with the publication of sensitive personal information about these innocent persons differs from one jurisdiction to another, as ascertained by variations in applicable restrictions on publication and disclosure of records throughout Canada. Many jurisdictions already provide for such protection by way of legislation. In jurisdictions where such restrictions are not put in place, judges are sometimes reluctant to post the full text of decisions on the internet. The Canadian Judicial Council addressed this issue in "Use of Personal

Information in Judgments and Recommended Protocol" (online: <http://www.cjc-ccm.gc.ca/article.asp?id=2811>).

With regard to the availability of search functions for judgments, it is recommended that courts provide the most powerful search functions available including, whenever possible, field search (e.g. by docket number, by date of judgment, by case name, etc.) and full text search. However, if the judgments are posted on the internet, it is a good practice to prevent indexing and cache storage from web robots or "spiders". Such indexation and cache storage of court information makes this information available even when the purpose of the search is not to find court records, as any judgment could be found unintentionally using popular search engines like Google or Yahoo. Moreover, when the judgment is cache stored by the search engine, it is available to internet users even if the court decides to withdraw the judgment from public access. To prevent such problems, very simple technical standards can be implemented (for further information, see the Robots exclusion protocol and the Robot Meta tag standard, online: <http://www.robotstxt.org/wc/exclusion.html>).

Note that courts may want to grant the same rights of access to some other types of court records which are of central importance to the open courts principle and which pose little risk to the privacy and security of individuals. This is addressed in Section 4.6.4 of this policy.

4.6.2 Docket Information

Members of the public shall have both on-site and, where available, remote access to docket information, provided that personal data identifiers are not made remotely accessible.

Discussion

The access policy should provide for broad public access to docket information, which is essential for ensuring the openness of court proceedings. However, given the fact that the docket may contain personal data identifiers, it is important that relevant docket information be accessible in a way that does not disclose at the same time such personal data identifiers.

Since there are many variations in Canada with regard to the content and management of docket information, in some situations technical and/or statutory changes will have to occur before providing the public with remote electronic access to docket information. In some courts, only small portions of the docket will first be made accessible, such as dates of hearings or basic case lists.

With regard to the availability of search functions for docket information, full text search is not usually required, and may not be appropriate. In most situations, search by docket number, names of parties and type of proceedings will suffice for the purposes closely linked with the rationale for open courts. It must be noted that many sets of information may also be accessed by way of lists of cases presented by date of hearing, party name or docket number, without having to provide a search engine to the user.

4.6.3 Case Files

Parties shall have both on-site and, where available, remote and registered access to their own case file. Members of the public shall only have on-site access to case files, unless otherwise provided in this access policy.

Discussion

Case files are the repositories of all documents pertaining to the court's cases. These documents include information such as personal data identifiers and other personally identifiable data, business proprietary information, details about financial situations and medical conditions of individuals, affidavits, exhibits, many of which are only partially relevant for the disposition of the case. The pleadings may also contain unsubstantiated and sometimes outrageous allegations, which may provide little assistance to the public's understanding of the judicial process or even be defamatory in nature. Consequently, there are many risks to individual and public rights and interests associated with unrestricted remote access to materials contained in the case file, and often unclear benefit with regard to the open courts principle.

The access policy should grant the parties with all available means of access to their own case file. However, as far as the public is concerned, access to such information should be limited to the court premises, except for those records that a specific court determines should be made remotely available to the public pursuant to Section 4.6.4, below, or for those persons who are granted extended access pursuant to Section 5, below.

Several jurisdictions have enacted statutory provisions that prohibit any public disclosure of certain sensitive materials found in case files such as financial statements or medical reports. For those jurisdictions where there is no such legal framework, it may be appropriate for courts to include similar restrictions in their access policy.

Not all documents in the case file will raise the same level of concern regarding remote public access. If any court wants to only grant remote public access to <u>part</u> of their case files then they can use Section 4.6.4, below, to list the types of documents for which this type of access is available.

4.6.4 Other Court Records

In addition to the records already listed in this policy, members of the public shall have remote access, where available, to those court records, or portions thereof, listed in this subsection.

Discussion

This subsection of this model policy contemplates the possibility that specific courts may determine that some types of records can be made remotely available to the public without engaging serious risks to individual privacy, security, or to the proper administration of justice. If a specific court makes such distinctions between types of court records, then their policy should contain subsections listing those records. If a specific court does not make such distinctions, then this subsection is not needed.

5 Extended Access

5.1 Request for Extended Access

Any member of the public may make a request for access to a portion of the court record that is otherwise restricted pursuant to this policy. The request shall be made in the form prescribed by the court. In deciding whether or not access should be granted, and what specific terms and conditions should be imposed, including the possibility of registered access, the following criteria shall be taken into consideration:

a) **the connection between the purposes for which access is sought and the rationale for the constitutional right to open courts;**
b) **the potential detrimental impact on the rights of individuals and on the proper administration of justice, if the request is granted; and**
c) **the adequacy of existing legal or non-legal norms, and remedies for their breach, if improper use is made of the information contained in the court records to which access is granted. This includes, but is not restricted to, existing privacy laws and professional norms such as journalistic ethics.**

Discussion

The access policy should be adaptable to the particular needs of certain members of the public. When a member of the public seeks access to court records by means that are not otherwise granted in Section 4, above, the court should be able to respond in a timely way to administrative requests for extended access. Such requests will typically be made by individuals who have a professional interest in accessing court record information with minimal restrictions, such as journalists and researchers, but any member of the public should be able to make a request.

When granted, extended access will typically be governed by an "access agreement". Such an agreement may include terms and conditions primarily designed to minimize the risks that extended access will be used to undermine the privacy and security rights of individuals or the proper administration of justice. Such terms and conditions could provide for the rights and obligations of the user regarding registered access, applicable fees, etc. If remote electronic access to case files is granted, a provision prohibiting massive downloading of files might be included.

Since it is foreseeable that certain categories of individuals will ask for extended access, such as academics, law researchers or journalists, the court may design boilerplate access agreements adapted to those categories of users.

5.2 Bulk Access

The court may permit bulk access to a portion or to the entirety of the court record. Such access shall be governed by a special agreement with the court that may include the requirement of registered access and should contain terms and conditions establishing that:

a) **the information should be regularly checked against the source of the court record for accuracy, if this information is to be published or re-distributed; and**
b) **any use of the information contained in the court record should comply with provincial and federal privacy and credit reporting legislation, as well as any other applicable law.**

Discussion

Bulk access is the ability to have systematic and direct access to all or to a significant subset of court record information or documents, including compiled information.

Courts may grant bulk access to individuals or to private or governmental organizations. The purpose for which the individual or organization needs this type of access may range from academic research to commercial publication. It is not recommended that bulk access be granted to individuals or organizations that are likely to use court record information in a manner that poses a serious risk to the privacy and security rights of participants in the judicial system and for purposes not connected with the open court principle.

Publishers of case law are traditionally granted bulk access to judgments, as their purpose is closely related to open access. Credit or insurance agencies, private investigators and information brokers may have a legitimate interest in bulk access not only to judgments, but also to case files, but they should be granted bulk access only in jurisdictions where their use of information is regulated in such a manner that does not undermine the proper administration of justice and the rights and interests of participants in judicial proceedings.

When granted, bulk access will typically be governed by an "access agreement", as is the case for the other types of extended access described in the previous subsection.

6 Information Management

6.1 Authentication and Security

The court shall put into place proper security, logging, archiving and audit functions for the management of court records.

Discussion

Proper security measures are paramount to ensure the integrity of information and documents that are created, stored, transferred, transmitted and otherwise managed by the court.

6.2 Destruction of Records

When court records are destroyed, the court shall implement proper methods and protocols to make sure that all of the information found in those records is not reusable.

Discussion

For paper records, the proper method of destruction is the paper shredder or other similar means. For digital documents, it is not always sufficient to only "delete" the file from the system, since such deleted information might nevertheless remain retrievable through special means. Before discarding any computer, hard drive or diskette, the court must put in place appropriate measures so that the information found on these supports is completely "wiped". It should be clear that "deleting" a digital record is not a proper method for making sure it is destroyed.

7 Policy Dissemination

The court shall inform the public and participants to the judicial system of the extent to which court record information is made available to the public, and of the measures that are taken pursuant to this policy to protect their personal information.

Discussion

When a person is entering into the judicial process, whether as a party or as a witness, this person should be informed of the key elements of the policy pertaining to their personal information. This could be achieved by providing them with a brochure summarizing the access policy. A particular emphasis must be made on the public availability of the documents that will be widely accessible through the internet, namely judgments. Short notices regarding the duties of litigants and their counsel with regard to the inclusion of personal information in the court record could also be included in statements of claim and forms prescribed by court rules. This is key to ensuring that all participants in judicial proceedings are made aware, and in some cases reassured, about the level of privacy protection they can expect.

8 Maintenance and Development

The court shall create a steering committee for the maintenance and further development of this policy. This committee should have representatives from each relevant court service and is responsible for various aspects of this policy's maintenance and development, including:

a) implementation;
b) dissemination;
c) seeking and receiving comments;
d) evaluation;
e) reviewing; and
f) recommending modifications.

Discussion

The policy must include guidelines to ensure its ongoing maintenance and development. It should be adapted to the court's specific environment, as that environment changes.

Bibliography – Selected Materials

Case Law

Attorney General (Nova Scotia) v. McIntyre, [1982] 1 S.C.R. 175.

Edmonton Journal v. Alberta (A.G.), [1989] 2 S.C.R. 1326.

Vickery v. Nova Scotia Supreme Court (Prothonotary), [1991] 1 S.C.R. 671.

Dagenais v. Canadian Broadcasting Corp., [1994] 3 S.C.R. 835.

Canadian Broadcasting Corp. v. New Brunswick (A.G.), [1996] 3 S.C.R. 480.

F.N. (Re), [2000] 1 S.C.R. 880, 2000 CSC 35.

R. v. Mentuck, [2001] 3 S.C.R. 442, 2001 SCC 76.

Sierra Club of Canada v. Canada (Minister of finance), [2002] S.C.R. 522, 2002 SCC 41.

Vancouver Sun (Re), [2004] 2 R.C.S. 332, 2004 CSC 43.

Articles

M. Fitz-James, "Defending the Publicness of the Justice System", in P. A. Molinari, ed., *Dialogues About Justice: The Public, legislators, courts and the Media* (Montreal, Canadian Institute for the Administration of Justice/Thémis, 2002) 107.

B. Givens, "Public records on the Internet: The Privacy Dilemma" (April 2002), Privacy Rights Clearinghouse, online: <http://www.privacyrights.org/ar/onlinepubrecs.htm>.

E.F. Judge, "Canada's Courts Online: Privacy, Public Access and Electronic Court Records" in P. A. Molinari, ed., *Dialogues About Justice: The Public, legislators, courts and the Media* (Montreal, Canadian Institute for the Administration of Justice/Thémis, 2002) 1.

Reporters Committee for Freedom of the Press, "Electronic Access to Court Records: Ensuring Access in the Public Interest", online: <http://www.rcfp.org/courtaccess/index.html>.

A. Wallace, "Courts Online - Privacy and Public Access in Australian and United States' Courts" (2001), article written in support of a presentation given at CTC7, online: <http://www.ctc8.net/showarticle.asp?id=23>.

L. Webster, "Caught in Converging Technologies: The Modern Court Administrator and the Privacy/Access/Security Conundrum" (1999), article written in support of a presentation given at CTC6, online: <http://www.ctc8.net/showarticle.asp?id=39>.

Policy Materials

D.I. Brenner & J. Hoffman, “Electronic Filing, Access to Court Records and Privacy” (March 2002), Canadian Judicial Council.

Judges Technology Advisory Committee, “Discussion Paper on Open Courts, Electronic Access to Court Records, and Privacy” (May 2003), Canadian Judicial Council, online: <http://www.cjc-ccm.gc.ca/cmslib/general/OpenCourts-2-EN.pdf>.

Justice Québec, « Analyse préliminaire du Système intégré d’information de justice », (May 2003), online: <http://www.justice.gouv.qc.ca/francais/publications/rapports/siij-analyse.htm>.

Minnesota Supreme Court, “Recommendations of the Minnesota Supreme Court Advisory Committee on Rules of Public Access to Records of the Judicial Branch - Final Report” (June 2004), Minnesota Judicial Branch, online: <http://www.courts.state.mn.us/cio/public_notices/accessreport.htm>.

New York State - Commission on Public Access to Court Records, “Report to the Chief Judge of the State of New York”, (February 2004), online: <http://www.courtaccess.org/states/ny/documents/ny-report-publicaccess2004.pdf>.

K. Roche, “A Quiet Revolution in the Courts: Electronic Access to State Court Records” (October 2002), Center for Democracy & Technology, online: <http://www.ctd.org/publications/020821courtrecords.shtml>.

D. Roussel, *Modèle de pratiques de protection des renseignements personnels,* (Québec: Les Publications du Québec, 2004), online : <http://www.aiprp.gouv.qc.ca/autre/index.asp?Sect=Modele>.

M.W. Steketee & A. Carlson, “Developing CCJ/COSCA Guidelines for Public Access to Court Records: A National Project to Assist State Courts” (October 2002), National Center for State Courts / Justice Management Institute, online: <http://www.courtaccess.org/modelpolicy>.

Supreme Court of Florida, “Committee on Privacy and Court Records: Report and Recommendations” (Draft - May 6, 2005), online: <http://www.flcourts.org/gen_public/stratplan/privacy.shtml>.

Québec - Commission d’accès à l’information, « Avis de la Commission d'accès à l'information concernant le Système intégré d’information de justice (SIIJ) présenté par le ministère de la Justice », dossier 02 17 29 (January 2004), online: <http://www.cai.gouv.qc.ca/05_communiques_et_discours/01_pdf/a021729.pdf>

Treasury Board of Canada, “Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks” (August 2002), online: <http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld_e.asp>.

Appendix – Model Policy (Text Only)

Model Policy for Access to Court Records in Canada

1 General Provisions

1.1 Purpose

The purpose of this policy is to define principles of access to court records, consistent with applicable statutory and common law rules, so as to guide the judiciary in the exercise of its supervisory and protective power over court records. The principles stated in this policy are the result of a balancing of the constitutional requirement of open courts against other rights and interests of the public and participants to judicial proceedings, namely privacy and security of individuals and the proper administration of justice.

1.2 Scope and Application

1.2.1 Persons Covered

This policy sets out the principles governing the public's access to court records. It is not intended to apply to the availability of court records to the judiciary and court personnel.

1.2.2 Type of Proceeding

This policy applies to court records in both civil and criminal proceedings, at both trial and appeal levels, unless otherwise indicated.

1.2.3 Form of Court Record

This policy covers all court records in any form, whether these records are created, stored or made available on paper or in digital format.

1.2.4 Other Applicable Laws

The access provided for in this policy is subject to any applicable statutory or common law provision regarding access to, or publication of, court records.

1.3 Definitions

1.3.1 Access

"Access" means the ability to view and to obtain a copy of a court record.

1.3.2 Case File

"Case file" refers to docket information and documents in connection with a single judicial proceeding, such as pleadings, indictments, exhibits, warrants and judgments.

1.3.3 Court Record

"Court record" includes any information or document that is collected, received, stored, maintained or archived by a court in connection with its judicial proceedings. It includes, but is not limited to:

a) case files;
b) dockets;
c) minute books;
d) calendars of hearings;
e) case indexes;
f) registers of actions; and
g) records of the proceedings in any form.

This definition does not include other records that might be maintained by court staff, but that are not connected with court proceedings, such as license and public land records. It does not include any information that merely pertains to management and administration of the court, such as judicial training programs, scheduling of judges and trials and statistics of judicial activity. Neither does it include any personal note, memorandum, draft and similar document or information that is prepared and used by judges, court officials and other court personnel.

1.3.4 Docket

"Docket" means a data system in which court staff collect and store information about each proceeding initiated before the court, such as:

a) information about the court division and type of case;
b) docket number;
c) names and roles of parties;
d) names of counsel or solicitors of record;
e) names of judges and judicial officers;
f) nature of proceedings, including cause of action or criminal informations and indictments;
g) information about the requested relief or amount of damages;
h) list and corresponding filing dates of documents present in the case file;
i) dates of hearings; and
j) dispositions with their corresponding dates.

1.3.5 Judgment

"Judgment" refers to any decision rendered by judges or judicial officers, including endorsements and orders, as well as any disposition or reasons given in connection with such decision.

1.3.6 Parties

"Parties" include the parties, their counsel and other authorized agents.

1.3.7 Personal data identifiers

"Personal data identifiers" refers to personal information that, when combined together or with the name of an individual, enables the direct identification of this individual so as to pose a serious threat to this individual's personal security. This information includes:

a) **day and month of birth;**
b) **addresses (e.g. civic, postal or e-mail);**
c) **unique numbers (e.g. phone, social insurance, financial accounts); and**
d) **biometrical information (e.g. fingerprints, facial image).**

"Personal data identifiers" does not include a person's name.

1.3.8 Personal Information

"Personal information" is information about an identifiable individual.

1.3.9 Registered Access

"Registered Access" is a means of access that entails identification of the person who is granted certain rights of access. This means of access may also involve the logging of requests made by this person during a session.

1.3.10 Remote Access

"Remote access" means the ability to access court records without having to be physically present where the records are kept, and without needing the assistance of court personnel.

2 Creation

2.1 Inclusion of Personal Information

Rules that govern the filing of documents in the court record shall prohibit the inclusion of unnecessary personal data identifiers and other personal information in the court record. Such information shall be included only when required for the disposition of the

case and, when possible, only at the moment this information needs to be part of the court record.

2.2 Responsibilities of the Parties

When the parties prepare pleadings, indictments and other documents that are intended to be part of the case file, they are responsible for limiting the disclosure of personal data identifiers and other personal information to what is necessary for the disposition of the case.

2.3 Responsibilities of the Judiciary

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.

3 Storage

When storing court records, the court should ensure, where possible, that personal data identifiers and other personal information that should not be disclosed to the public are capable of being segregated from other documents or information found in the court record.

4 Access

4.1 Presumption of Access

Members of the public have presumptive right of access to all court records.

4.2 Fees

Fees should not impede access under this policy.

4.3 Existence of a Case File

Members of the public are entitled to know that a case file exists, even when a case file is sealed or subject to a non-publication order.

4.4 Format of Records

Members of the public are entitled to access court records in the format in which they are maintained.

4.5 Search Functions

When accessing court records, members of the public shall be provided with appropriate search functions that allow for efficient research of court records but also limit the risk of improper use of personal information.

4.6 Type of Record and Means of Access

4.6.1 Judgments

Members of the public shall have on-site access and, where available, remote access to all judgments.

4.6.2 Docket Information

Members of the public shall have both on-site and, where available, remote access to docket information, provided that personal data identifiers are not made remotely accessible.

4.6.3 Case Files

Parties shall have both on-site and, where available, remote and registered access to their own case file. Members of the public shall only have on-site access to case files, unless otherwise provided in this access policy.

4.6.4 Other Court Records

In addition to the records already listed in this policy, members of the public shall have remote access, where available, to those court records, or portions thereof, listed in this subsection.

5 Extended Access

5.1 Request for Extended Access

Any member of the public may make a request for access to a portion of the court record that is otherwise restricted pursuant to this policy. The request shall be made in the form prescribed by the court. In deciding whether or not access should be granted, and what specific terms and conditions should be imposed, including the possibility of registered access, the following criteria shall be taken into consideration:

- **a) the connection between the purposes for which access is sought and the rationale for the constitutional right to open courts;**
- **b) the potential detrimental impact on the rights of individuals and on the proper administration of justice, if the request is granted; and**
- **c) the adequacy of existing legal or non-legal norms, and remedies for their breach, if improper use is made of the information contained in the court**

records to which access is granted. This includes, but is not restricted to, existing privacy laws and professional norms such as journalistic ethics.

5.2 Bulk Access

The court may permit bulk access to a portion or to the entirety of the court record. Such access shall be governed by a special agreement with the court that may include the requirement of registered access and should contain terms and conditions establishing that:

a) **the information should be regularly checked against the source of the court record for accuracy, if this information is to be published or re-distributed; and**
b) **any use of the information contained in the court record should comply with provincial and federal privacy and credit reporting legislation, as well as any other applicable law.**

6 Information Management

6.1 Authentication and Security

The court shall put into place proper security, logging, archiving and audit functions for the management of court records.

6.2 Destruction of Records

When court records are destroyed, the court shall implement proper methods and protocols to make sure that all of the information found in those records is not reusable.

7 Policy Dissemination

The court shall inform the public and participants to the judicial system of the extent to which court record information is made available to the public, and of the measures that are taken pursuant to this policy to protect their personal information.

8 Maintenance and Development

The court shall create a steering committee for the maintenance and further development of this policy. This committee should have representatives from each relevant court service and is responsible for various aspects of this policy's maintenance and development, including:

a) **implementation;**
b) **dissemination;**
c) **seeking and receiving comments;**
d) **evaluation;**
e) **reviewing; and**
f) **recommending modifications.**