Canadian Judicial Council

COURT INFORMATION MANAGEMENT

POLICY FRAMEWORK TO ACCOMMODATE THE DIGITAL ENVIRONMENT

Discussion Paper

Prepared by Jo Sherman
For the Canadian Judicial Council

© Canadian Judicial Council
Catalogue Number JU14-23/2013E-PDF
ISBN 978-1-100-21993-6

Available from:
Canadian Judicial Council
Ottawa, Ontario
K1A 0W8
(613) 288-1566
(613) 288-1575 (facsimile)
and at: www.cjc-ccm.gc.ca

FOREWORD

Traditionally, courts have relied on the availability of filed documents – both paper based or electronic – as a means to move the work of the Court forward. Recent technological advancements have dramatically improved the way documents are captured, stored, shared and retrieved electronically. Managing this information and making full use of digital technology has been a challenge for all institutions, including the courts. The possibility of having instant access to digitized documents from virtually anywhere presents enormous benefits; however, there are also risks in allowing unfettered access to court documents. Some information is sensitive and the impact of its release needs to be carefully weighed in the context of ensuring a fair trial and protecting vulnerable individuals. Courts also have a duty to protect the integrity of all information that are part of legal proceedings.

As expectations grow that courts will foster ongoing transparency through the use of modern information technology, courts must seize the opportunities to streamline their policies and governance in this regard. By setting definitions, architectural principles and information management policies, courts may approach this evolving issue with confidence. This discussion paper proposes a framework for individual courts to consider when moving towards the development of their respective Information Management policies.

The discussion paper has been prepared by the Canadian Judicial Council's technology committee. While it should not be considered as a policy of the Council, it provides an excellent starting point for courts to reflect on the challenges and opportunities offered by modern information technology in framing their own policies.

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

This paper proposes a framework and methodology for information management policy formulation within courts.

It is designed to enable court policy makers to embrace the opportunities presented by our networked society while also accommodating the emerging risks. The approach recommended in this paper also provides those responsible for the architecture design and implementation of court information systems with a policy foundation to underpin and guide their work.

The policy framework addresses the following areas:

- Foundational Policies
- Access Policies
- Privacy Policies
- Security Policies
- Preservation Policies
- Performance Measurement Policies

It also proposes definitions for the following key terms:

- Judicial Information
- Private Judicial Information
- Court Judicial Information
- Case File (Restricted Access Information)
- Court Record (Open Access Information)
- Court Docket
- Personal Information

The recommended methodology within each jurisdiction is to:

1. Confirm recommended key definitions (Appendix 3)
2. Complete an Allocation Table for the ***Court Record*** and ***Case File*** (Appendix 2)

3. Develop an Access to Court Information Table to define who should have access to what information for each ***Case Type*** (Appendix 2)
4. Review the recommended policies (Section 8) in terms of suitability for local application taking into account any unique characteristics or requirements within the jurisdiction and adjusting them as required to accommodate any pre-existing legislative or similar constraints.

Once these steps have been performed the emerging information management policies will provide a set of Architectural Principles to guide those responsible for court computer system design.

Modern approaches to computer system design, such as Service Oriented Architecture ("SOA"), present significant opportunities to implement information management policies within court case management systems in a way that preserves independence of separate systems while facilitating the necessary interoperability and information exchange that is necessary to support an effective justice system. For this reason, it is proposed as a suitable approach for large scale court system development initiatives.

2 INTRODUCTION

2.1 Terms of Reference

This paper was commissioned by the Canadian Judicial Council. At a meeting of the Technology Sub-Committee in May 2011, a broad range of issues were discussed in relation to this paper and it was resolved that the final deliverable should be to:

- Deliver an Information Management Policy framework for Canadian Courts to accommodate the risks, challenges and opportunities of a networked society and the increasing prevalence of court information in digitized format.
- Develop these policies to address issues such as access, privacy, security, preservation and performance measurement and control and ensure that all policies are aligned with broader 'core values' for courts.
- Propose foundational definitions (e.g. Court Record, Case File etc) to facilitate a common understanding and to ensure consistent terminology is used across all policies.
- Ensure that the policies are suitable for use as Architectural Principles to guide the design of future court information systems.
- Provide a policy framework that preserves judicial control over Court Records.

2.2 Our Networked Society

We are experiencing astounding technological change that is bringing about a worldwide upheaval in the way we communicate and exchange information. Social networking tools have rapidly emerged over recent years to infiltrate our personal and professional interactions. Anyone with Internet access is now free to instantaneously publish to the world at large. Even uncensored, unreliable and scandalous information can be so disseminated. Over recent months, through the Wikileaks incident, we have seen a groundswell of support for open access to sensitive government information from a large proportion of the international on-line community. This incident is, at the same time, considered by others to be no more than a renegade effort by a few rogue individuals to bring about institutional embarrassment through exposure of highly sensitive information. Even the United States government, applying the full arsenal of its legal system has struggled to effectively respond to such an incident.

In line with this, large organizations worldwide are now investing heavily in '*reputation management*' to counteract the potential damage that can be caused by embarrassing on-line leaks or unauthorised exposure of sensitive internal information. Courts too need to contemplate these potential risks.

It is now possible for anyone to publish defamatory and unreliable information through websites, email blasts, blogs, and Twitter. Mass publication tools, are also profoundly changing the way we interact within our business and social communities. The traditional boundaries between our professional and private lives are now becoming blurred as work and personal networks merge.

This new world order is virtual, dynamic and organic. Our networked society can facilitate widespread collaboration or rebellion across what would have traditionally been geographic or jurisdictional barriers.

This is also an era of exponential growth in the volume of personal information that may be shared, captured, mined, disseminated and exposed whether purposefully, inadvertently or maliciously through on-line computer systems. The consequential invasion of privacy rights that inevitably and frequently occurs can lead to personal distress, fraud, identity theft or risks to personal safety.

This changing social and commercial landscape is challenging traditional information management philosophies. All over the world owners, producers, distributors, publishers, custodians, aggregators and consumers of information are confronting the new order. Some are closing their eyes to it while others are exploiting it. Governments are particularly challenged and the legislature is in many cases, even further behind, desperately chasing a horse that, to a large extent, has already bolted.

2.3 The Challenge for Courts : New Policy Formulation

Courts too, need to contemplate the ramifications of these universal developments. It is becoming increasingly apparent that there are many compelling opportunities now emerging for the judiciary to take a leadership role in formulating important new information management policies in this relatively unchartered territory.

This will require a rethink of our traditional paper based perspectives in relation to *access, control, privacy, security* and other key information management concepts that need to be recast to accommodate the new reality.

Strategies must be developed to ensure that courts embrace opportunities and minimise new risks that did not present themselves in our paper based world and are unique to the digital environment. Many of the new opportunities and risks relate to the management, or *mis*management, of court information. There is now significant potential for the core values that underpin our justice system such as fairness, transparency, integrity and independence, to be inadvertently impacted by inadequate policy development in this domain.

2.4 Purpose of this Document

This discussion paper contains a proposed Information Management Policy Framework for Canadian courts to accommodate new challenges in our networked society.

3 ELECTRONIC COURT INFORMATION

The increasing prevalence of information technology in the justice domain has brought about significant changes in the way court information is structured, captured, stored, accessed, maintained, distributed, secured and preserved. These changes are challenging traditional information management policies and practices that are intrinsically based on a paper paradigm.

Before effective new information management policies can be formulated however, the significant differences between paper and electronic information must be considered alongside the unique challenges of our new digitized environment.

3.1 Documents versus Information

Whereas a traditional court file comprised a number of documents, a modern court file will contain a large number of information fields that may be sourced from and dispersed across a variety of different locations. It is more *granular* in that it needs to be considered in terms of the many separate components of information that reside within it.

Electronic copies of the file or components within it may reside in multiple replicated locations within and external to the court and the notion of control over the file is much more difficult to translate into the digital domain due to this fragmentation, distribution and duplication of information.

Further complexity arises from the fact that today's court files are comprised of a collection of distinct information components or fields of data that are held in case management database systems rather than in documents on a paper file. It is now possible to manage and exchange 'fields of information' rather than capturing the information within paper 'documents'. For this reason, court rules, practice directives and policies surrounding management of court information need to focus increasingly on *information* rather than *documents*.

3.2 Practical Obscurity

A further key difference between paper and digital records is the fact that paper records by their nature provide "practical obscurity" of the information contained within them because anyone who wishes to peruse a court file has to travel to the physical location of the paper file in order to access it.

This presents a natural barrier to access because it is rarely cost and time effective for anyone other than the parties or other persons directly involved in the case to go to such lengths. Electronic information, on the other hand, may be easily disseminated via the Internet anywhere and anytime at a very low cost therefore making it easily accessible to the world at large.

3.3 Possession and Control

Developing policy and implementing technology surrounding the ownership and control of court information is not as simple in the digital domain as it was in a paper based world.

In a traditional court environment the 'official court record' is generally held in paper files located in courthouses under the *physical* control of the judiciary.

It has, in most jurisdictions, been the judiciary who determined who will have access to court information and the terms surrounding that access. Such arrangements are often documented in policy materials or procedural guidelines that may also involve a degree of judicial discretion.

In the tangible, paper based world criminal justice files were physically delivered or transferred from one agency to another as a file progressed through the justice system, however; while the 'file' was physically located within the court it was under the care and control of the judiciary.

In a paper based world *possession* of a court file is synonymous with *control* over that file. It was easy for the judiciary to *control* Case Files in such an environment because an original court file could only reside in one physical location at a time and those with possession of the physical file could easily control the ways in which information within it could be accessed.

In the digital domain however, it is quite possible to have possession of information without control and conversely, it is possible to have control of information without physical possession.

Commercial databases accessible via the Internet are one of the best examples of this. As a customer of a bank you can control the transactions on your 'file' even though you don't have physical possession of the server upon which the information resides. Control doesn't require possession and possession doesn't necessarily deliver control.

The concept of control in relation to electronic court records therefore needs to move away from traditional notions that are linked to physical possession. Locating a server within a courthouse will not necessarily deliver control over its contents to the judiciary who work within that building. Conversely, if appropriate governance arrangements and safeguards are established, it may be possible to exercise control over court information residing in remote hardware.

3.4 Custodianship

These paper based concepts are being progressively challenged as we approach virtual models of electronic information management and new concepts such as information 'custodianship' have emerged as a consequence.

The notion of custodianship is particularly relevant to a court's responsibility and duty to safeguard the interests of those affected by court records.

Indeed, courts are generally recognized as having a supervisory duty and protective power over court records. See *A.G. (Nova Scotia) v. MacIntyre*, [1982] 1 S.C.R. 175, and other Supreme Court decisions citing it. Some degree of custodianship or guardianship seems to be a part of that concept.

3.5 Architecture requires Information Management Policy

In many jurisdictions it is increasingly necessary to find effective new ways to implement control over electronic court records to establish the same controls that were available when they were held in paper format. This requires a shift of focus away from physicality and presence towards the development of policies that not only guide operational practice but can also be, implemented within and enforced by technology architecture that underpins our court systems. The policy framework behind this must be proactively developed by the judiciary to address cornerstone issues such as access, privacy and security.

The determination of who should have access to information held on court files involves a consideration of not only access and transparency issues but also a consideration of the broader interests of effective justice administration, freedom of expression, the need to protect vulnerable persons and sensitive personal information.

The architects of court information systems may then propose a range of technical infrastructure options that support the information management policies, for example, relating to where and how data should be hosted, how it should be accessed, with whom it will be shared and how it will be protected.

Ultimately, the preferred architectural solution for any new court information system should be selected by a governance group comprising judicial representation. This group will need to consider recommendations from architects, and a cost, benefit and risk analysis in relation to each option. The extent to which each option aligns with the pre-defined information management policies will, of course, be a paramount consideration.

Sound governance surrounding the information management policies must also be established to ensure that they are well communicated within and external to the court and that policy continues to adapt to meet evolving needs. Independent audit arrangements in relation to technology system designs will also be necessary to ensure that the endorsed policies are effectively implemented in new systems.

There is, however, a very important caveat that must be put forward in relation to these broad propositions. That is; a policy framework will only be an effective mechanism if it is actually applied in practice. It must be understood and adopted by those responsible for implementation and it needs to be adhered to and governed on an ongoing basis. If it holds no more than platitude status and is shelved or sidelined by those responsible for implementation then it will be a totally ineffective conduit through which core values may be supported and judicial controls preserved.

As a related point, in a court environment where the judicial policy makers have limited confidence that their court information management policy decisions will be properly embraced by those responsible for implementation of new information systems, a more tangible, restrictive and traditional approach to establishing control may be necessary. This is likely to incorporate and emphasise physical possession in order to maintain judicial confidence.

4 NEW RISKS IN OUR DIGITIZED SOCIETY

As courts all over the world re-define their roles in an increasingly networked and digitized society, many new challenges, risks and opportunities will be encountered that were not present in the paper based world. New information management policies need to be developed and then implemented in court information systems to embrace such opportunities, address the challenges and mitigate the risks. Some of these are canvassed below.

4.1 It is impossible to control information once it's released on the Internet.

Once electronic court information has been released, particularly via the Internet, it can potentially be accessed, aggregated, collated, mined, repackaged, disseminated and commercialized by persons or organizations with no authority to do so, nor commitment, contractual or otherwise, to maintain its quality or to ensure it is effectively and accurately represented. This could potentially, over time, erode the integrity of our legal system and may reduce public confidence in the courts.

4.2 It is easy for a court to lose control over the quality of its information

There are often inadequate publication and distribution constraints and quality control checks established in formal or contractual arrangements surrounding bulk access and distribution by third parties (e.g. distributors, publishers, brokers). Some courts have effectively lost control of important data due to exclusive arrangements that have been established with commercial information brokers that involve, for example, external hosting of electronically filed documents without effective data repatriation provisions or quality control checks.

4.3 Data mining may facilitate unauthorised bulk-access to court information

It is possible for unauthorized aggregators, data miners and distributors to obtain unauthorised bulk access to electronic court information and to re-package and distribute it for commercial gain without any safeguards to ensure the information is properly presented and its integrity is preserved. This dissemination of unreliable court information could potentially erode confidence in the legal system.

4.4 Risks to vulnerable people

Unlimited access to on-line court information may increase personal safety risks for vulnerable people. This is particularly a concern in criminal and family law cases and in cases involving juvenile justice. Personal information relating to witnesses, jurors, victims of crime, troubled youths and children at risk will often need to be protected from public access to minimise the potential for them to be exposed to harm. If this consideration is not accommodated in systems that deliver court information on-line, the risks can be greater than they were in the traditional paper based world due to the ease with which the information can be accessed by anyone with Internet access.

Confidentiality in relation to personal information will be a paramount policy consideration that will generally override the public's right to access where there is such a potential increased risk to personal safety. Protection of vulnerable people is a particularly important overriding consideration when weighed up against competing values such as the community's right to access information on court files.

Young offender records and other sensitive records relating to vulnerable people can inadvertently become inappropriately distributed and accessible in some integrated justice information system programs where there is a loss of control as data flows 'downstream' into other justice agencies. Mitigation of such risks needs to be built into the architecture design of such systems.

In the family law case of *Director of Child and Family Services v. D.M.P. et al*, 2009 MBQB 193 (CanLII)[1] a media reporter was banned from attending and reporting upon the proceedings largely because he had been twittering live feeds to the Internet during courtroom proceedings, despite instructions from the bench not to do so. Rivoalen J considered that his actions had caused potential harm to the child and held that the protection and welfare of a child superseded the interests of the media to obtain access to the courtroom.

4.5 Personal privacy may be invaded by persons with 'no right to know'

Broad, unrestricted access to court information can facilitate 'busy-body' enquiries and privacy violations due to the removal of practical obscurity barriers that are prevalent in a physical, paper based world.

The Supreme Court of Canada has long recognized privacy as an interest protected by both the common law and the Canadian Charter of Rights and Freedoms.[2] The US Supreme Court, likewise, has conferred constitutional status on certain aspects of privacy[3] and US federal trial courts have held that a victim's privacy rights are capable of overriding the principle that the judicial system ought to be fully open.[4] In New Zealand, the High Court has reached a similar conclusion[5] and the British Parliament attempted to regulate access to "protected material" on the grounds of privacy protection as early as 1997 in sexual offence proceedings.[6]

---

1 http://www.canlii.org/en/mb/mbqb/doc/2009/2009mbqb193/2009mbqb193.html

2 R v Beharriell (1995), 103 C.C.C. (3d) 92 (S.C.C.). per L'Heureux-Dubé J pp 124-125

3 Roe v Wade 410 U.S. 113 (1973)

4 In re Application of KSTP Television, 504 F. Supp. 360 (D. Minn. 1980).

5 Police v. O'Connor, [1992] 1 N.Z.L.R. 87 (H.C.), at p. 98.

6 "Protected material" including the victim's statement, a photograph of the victim, and the victim's medical report: Sexual Offences (Protected Material) Act 1997.

On-line court information systems can permit serious privacy violations where the architects who designed them fail to implement these important rights within the technology security framework.

4.6 Increased risk of identity theft, harassment, fraud

Broad access to court information without adequate protection of personal information may facilitate identity theft, harassment or fraud where personal details are inadvertently or purposefully embedded within the accessible information.

4.7 Access to disturbing material may cause distress or harm

Criminal Case Files often contain disturbing photo or video evidence that can cause distress or even harm to those who become exposed to it whether inadvertently or otherwise. It is easier for casual browsers who have no connection to such a case to either accidentally or purposefully view such material where on-line access arrangements are too liberally applied to information presented in court.

> *"One concern we had was that if family members were present in court we knew the impact on them would be irrevocable. They would not recover...*
>
> *Many photographs .. were not shown in court .. they'd be too disturbing for the public to view"*[7]

In the case of 'horrific' evidence (for example, contained in videotapes associated with sexual offences), a number of factors may need to be weighed when considering public access rights. These include[8]:

a) The nature and content of the evidence and, in particular, whether it depicts violent or degrading non-consensual sexual activity involving an identifiable victim.

b) The use to which the evidence will be put: will it advance a public interest, or is it intended primarily to satisfy prurient curiosity?

c) Whether innocent victims could be re-victimized through public dissemination of the evidence?

d) Would public dissemination amount to a significant violation of a victim's personal privacy, or will it simply result in embarrassment or discomfort?

e) Is there a reasonable basis to believe that possession of the evidence by a member of the public, including the media, could constitute a criminal offence such as possession (or publication) of child pornography?

---

[7] Canadian Lawyer Journal Article by Rob Tripp "Behind the Scenes" – January 2011 page 31. Quote from Michael Edelson, Edelson Clifford D'Angelo Barristers LLP, counsel for the accused in the recent high profile criminal trial of R v Russell Williams before Scott J,

[8] Horrific Video Tapes as Evidence: Balancing Open Court and Victim's Privacy – Bruce A. MacFarlane, Q.C. Deputy Minister of Justice Deputy Attorney General for the Province of Manitoba September 25th, 1998 [Originally published in 41 Criminal Law Quarterly 413 (1999)] http://www.canadiancriminallaw.com/articles/articles%20pdf/Horrific_Video_Tapes_as_Evidence.pdf

f) Was the evidence played or shown fully in court, or were there limitations imposed by the judge?

g) Whether the victim or their family members are likely to suffer long-term psychological or emotional injury if the evidence is made public?

h) Was the evidence ruled inadmissible at the trial and, if it was, did its exclusion result in or contribute to an acquittal?

i) Could a denial of access in any way prevent prejudice to the accused's right to a fair trial in any future proceedings?

This balancing exercise was undertaken by Watt J in *R v. Blencowe* (1997) 118 CCC (3d) 529 (Ont. Ct. (Gen Div)) where his honour endeavoured to strike a balance between the accused's right to a fair trial, including disclosure of evidence, and the privacy rights of the child victims depicted in the videotape evidence.

4.8 Fair trials are easily compromised

Fair trials may be compromised where smart phones or laptops are used in the courtroom to instantaneously transmit stories and pictures to the Internet. Orders excluding witnesses from the courtroom to preserve integrity of their evidence, may be circumvented if courtroom events or earlier testimony material are relayed to the Internet, for example, via Twitter or live Blogs.

> *"If you have instantaneous communication of the evidence, this means that all subsequent witnesses have access to the evidence in court as it's unfolding. It renders the traditional witness exclusion order worthless .. I would like to see our rules of practice amended to give judges and lawyers clear guidance.. "*[9]

The Supreme Court of the United Kingdom recently released a policy statement regarding "The Use of Live Text-Based Communications from Court"[10] The policy allows any member of a legal team or member of the public to use text-based communications from court, providing

(i) these are silent; and

(ii) there is no disruption to the proceedings in court."

The policy also stipulates that no one present in a courtroom is permitted to use a mobile device to make or receive a telephone call and provides that reporting restrictions may be put in place by the court in which case live text-based communications which makes information about proceedings public will not be permitted.

[9] ibid., p 28, see also R v Harry O'Brien (before Cunningham ACJ) – regarding the use of Twitter from the courtroom

[10] http://www.supremecourt.gov.uk/docs/live-text-based-comms.pdf

The policy further states that in a case involving a child, where anonymity is of the essence, text-based communications will be permitted, but any breach of the anonymity will be treated as a contempt of court. This policy is also discussed on slaw.ca. [11]

While this UK policy is quite liberal, the fact that it relates only to an appellate court is an important consideration because there are no jurors nor witnesses before the court, hence a reduced risk of inappropriate usage.

By sharp contrast, in February 2011, British Columbia's Provincial Court expressly banned Twitter, email and texting from inside courtrooms. The rationale for this was articulated to be the potential interference that may impact transcribing equipment rather than the potential for it to present a miscarriage of justice in the trial. In response to this development, BC Civil Liberties Association president, Rob Holmes said;[12]

> *"..as long as the courts aren't being disrupted, the public should be allowed to communicate from within the courtrooms.*
>
> *Clamping down on the ability of people unobtrusively to be able to communicate to others outside the courtroom what's going on inside the courtroom amounts to a denial of the open court principle.*
>
> *Everybody involved in the judicial system has to realize that they are the people's court. The people have a right to access to them."*

It is suggested that this perspective fails to accommodate the balancing perspective regarding potential risks to the conduct of a fair trial that may arise where unlimited usage of communication technologies is permitted from the courtroom.

Perhaps the key consideration should be; whether or not the usage of such communication technologies will compromise the effective administration of justice during the trial in the circumstances of the case at hand. Even Holmes puts forward the caveat that "as long as the courts aren't being disrupted" and the requirement for "unobtrusive" communication.

Of greater concern perhaps is the problem of juror indiscretion threatening a miscarriage of justice with the social phenomenon of jurors sharing information on-line. England's Chief Justice, Lord Judge, recently decried the "misuse" of the Internet by jurors, warning that it must stop if the jury system is to survive.[13]

Jurors have been known to seek suggestions from Facebook friends on how to vote, tweet about the perceived guilt or innocence of the accused and check out crime scenes on Google Earth.[14]

---

[11] http://www.slaw.ca/2011/02/03/uk-supreme-court-policy-on-tweeting-etc-from-court/

[12] http://www.theprovince.com/news/tweets+allowed+provincial+court+bans+Twitter+email+texting/4343454/story.html

[13] http://www.theprovince.com/technology/Tweeting+jurors+pose+threat+fair+trial/4082061/story.html#ixzz1Hzkoqc00

[14] http://www.canada.com/Innocent+until+tweeted+social+media+tests+rules+jury+trials/4080425/story.html

4.9 It's easier to leak sensitive court information and its impact is more damaging

The reputation of the judiciary may be compromised and public confidence in the court may be negatively impacted through publication of damaging, sensitive, embarrassing or inaccurate court information. It is now much easier for a disgruntled ex-employee, participant in the justice system, or member of the general public to publish such information instantaneously to millions of people via the Internet, wiki-leaks style.

4.10 Outsourcing eLodgment to commercial providers can lead to loss of control

Many international courts and justice departments have entered into commercial electronic lodgment arrangements with publishers or distributors which have inadvertently lead to a loss of control over their own court information. These arrangements often involve the establishment of document repositories that are managed by commercial providers outside the court's network and control. Such repositories can capture documents filed by litigants or their legal representatives and pleadings. In some cases courts have entered into such arrangements without adequate safeguards in terms of retrieval and access to their own documents and commercial third parties have been free to commercialize the content in any way they choose.

4.11 Outsourcing or 'cloud' arrangements can mean loss of control

The emerging trend to outsource data to reside on remote hosting servers that may be located across the border in foreign jurisdictions or in the "cloud" may appeal to court administrators managing tight budgets. However, these services can present significant risks if no safeguards are put in place to protect and secure data, to establish disaster recovery and data repatriation arrangements, and to ensure that privacy obligations are properly addressed. If data is actually hosted in a remote jurisdiction with limited privacy laws, it may not be possible to adequately implement the necessary technical arrangements to comply with the local obligations.

4.12 Commercial litigation may go elsewhere

Where a court embraces an open access policy, the ease with which court information can potentially be accessed on-line by the media or general public may deter some civil litigants from pursuing resolution of their commercial disputes through the court system, opting instead for the relative privacy and confidentiality of alternative dispute resolution options.

If the commercial sector looses confidence in the courts as a viable dispute resolution option this will have significant social and economic impacts. One major repercussion for example, would be the lack of certainty surrounding commercial arrangements and negotiations due to the reduced body of precedent establishing the legal ground rules within the jurisdiction.

4.13 Technology can sometimes drive Policy (when it should be vice versa)

As courts embrace new information systems and technology opportunities it's important to *ensure that the tail doesn't wag the dog*. While policy needs to be informed by the possibilities and risks associated with the technology of the day, it's important to ensure that policy directs technology solutions and not vice versa.

In the absence of clearly documented information management policies, architects charged with the responsibility to design and implement new information systems will sometimes make incorrect assumptions or may, at times, feel understandably compelled to make important strategic business decisions themselves to fill a policy void.

Policy formulation in relation to court information is much more complex and arguably more important in the electronic domain than it was in the paper based world. Traditional notions of access, security, privacy and preservation need to be recast to accommodate digital realities. It is more important to 'get it right' upfront due to the inherent and significant new risks that we need to be mitigated and in light of the cost of retrofitting information management systems later in the event that we initially 'got it wrong'.

Once information management policies are formulated and aligned with core values, they operate as the *architectural principles* and provide a business context to guide those responsible for the design of future court information systems.

5 INFORMATION MANAGEMENT POLICIES IN CONTEXT

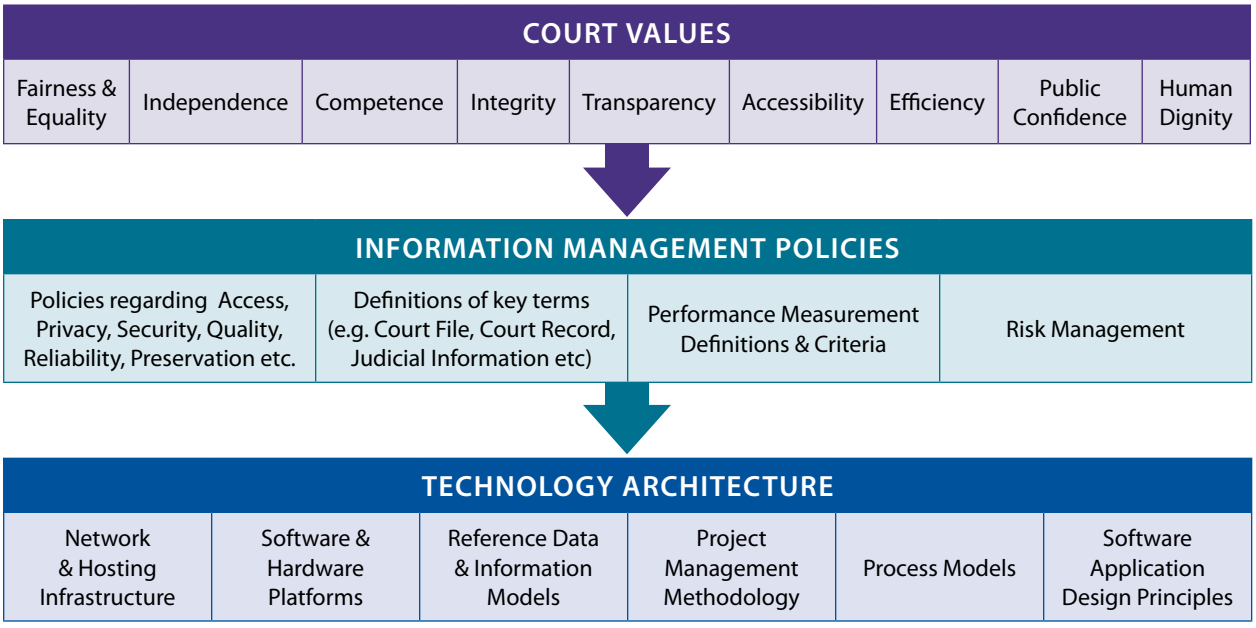
5.1 Inter-Relationships between Values, Policies and Architecture

The values of an organization are the core principles that provide its cultural foundation and guide behaviour. Strong leadership is required to ensure that values are effectively communicated, understood and infiltrated into all levels of organizational operations.

The values also provide a foundation upon which information management policy can be developed. It is these information management policies that in turn, provide guidance for the architects responsible for information system design and implementation.

These inter-relationships provide context and alignment for court information management policy formulation as shown in the diagram below.

Diagram 1: Inter-relationships between Values, Policies and Architecture



Any program of work involving large scale information system design and implementation or business improvement facilitated by technology will greatly benefit from a clearly articulated vision statement that succinctly describes the desired future state and is itself aligned with the organizational values. Alongside those values, the vision statement will also provide context for policy formulation. To that extent, program vision statements, if applicable, may be positioned between the policy layer and the values layer in the conceptual representation shown in the above diagram.

5.2 Core Values for Courts

The International Consortium for Court Excellence[15] has developed an *International Framework for Court Excellence*. This framework incorporates values, techniques and tools to improve the quality of court administration. The Consortium has agreed upon the following *core values* that underpin the effective functioning of a court:

- Equality;
- Fairness;
- Impartiality;
- Independence;
- Competence;
- Integrity;
- Transparency
- Accessibility
- Timeliness; and
- Certainty.

The framework is not prescriptive and can be adapted by any court to suit its own unique jurisdictional characteristics and requirements.

It could be argued that 'Certainty' could be excluded in so far as it is adequately accommodated within the other values. 'Timeliness' could also be replaced with 'Efficiency' to ensure that broader cost effectiveness elements would be captured, over and above the need to resolve disputes in a timely fashion.

The value of 'Public Confidence" might also be introduced. This is the cornerstone element within an effective justice system and, in a sense, it is actually an outcome that is only achieved as a result of the other values. If there is public confidence in the judicial system this will, in turn earn respect and trust from the community it serves.

Human dignity, liberty and respect for the individual are further concepts that might be considered candidate values. These are particularly important in an era that has progressively seen intrusion into the personal and private lives of citizens. Members of the community contemplating recourse to the courts or considering participation in the court process, for example by giving evidence or committing to jury duty, need to have confidence that their sensitive personal information will be treated carefully and with respect by the court.

---

[15] The International Consortium for Court Excellence comprises the Australasian Institute of Judicial Administration (AIJA), The Federal Judicial Center, The National Centre for State Courts (NCSC) and The Subordinate Courts of Singapore.

Ideally the core values embraced by a court will become integral to its culture and will guide behaviour of those working within it and the expectations of those interacting with it. In this regard the judiciary play a leadership role. The values should also be integrated into court policies, processes and automated systems and performance should be measured in accordance with them.

Clear and conscious articulation of court values serves to clearly convey to the community at large and to those who work within and interact with the justice system, the unique characteristics of courts particularly as compared with administrative arms of government.

The agreed core values must be infused into the culture and the operations of the court. Well articulated information policy pronouncements that are continuously monitored and communicated by the judicial leadership group provide a vehicle for this.

When encapsulated within well articulated information management policies, these values also provide an environmental context for the architects responsible for the design and implementation of new information technology systems. This, in turn, ensures that costly mistakes, resulting from misunderstanding or incorrect assumptions by those responsible for implementation, will be avoided.

5.3 Balancing Core Values

Open justice has long been regarded as a cornerstone of a democratic society. However, with the availability of new on-line channels through which access to court information may be broadly disseminated, it is now more important than ever to acknowledge that 'access' is not an absolute value that has no limits. In fact, curtailment of access to court information may be justifiable where there is a need to protect other important values that underpin an effective justice system.

The Canadian caselaw suggests that there is a strong presumption in favour of openness and that the burden to displace that presumption rests with the party seeking such displacement. This party must establish that, on the facts in the case, a restriction of access to court information is necessary for the proper administration of justice.

Frequently such requests to deny public access to court information will raise a number of competing rights, such as the accused's right to a fair trial and the victim's right to privacy.

A hierarchical approach to the consideration of such rights, weighing some over others, should be avoided. Instead, the court should strive to achieve a contextual balance that fully respects the importance of all values. Where a decision is taken to limit a right, the court's order should, as far as possible, minimize impairment of the right while serving the interest to be protected.

While it is often assumed that 'openness' will improve 'public confidence' in the courts, there are many circumstances where it can have the opposite effect. For example, those who are unwillingly and directly drawn into court proceedings, such as jurors, key witnesses and victims of crime will undoubtedly have increased confidence in the court if they know that their personal information, the circumstances surrounding their involvement and their expressed views will be respected and managed carefully by the court.

In the family law case of *Director of Child and Family Services v. D.M.P. et al*, 2009 MBQB 193 (CanLII)[16] Rivoalen J held that the protection and welfare of a child superseded the interests of the media to

[16] http://www.canlii.org/en/mb/mbqb/doc/2009/2009mbqb193/2009mbqb193.html

obtain access to the courtroom proceedings. Her honour quoted Chief Justice Scott in the *Canadian Broadcasting Corp. v. Manitoba (Attorney General)* decision where he said:

> *... Freedom of expression does not "trump other rights."*

then quoting from another Supreme Court of Canada decision:

> *... Although freedom of expression is undoubtedly a fundamental value, there are other fundamental values that are also deserving of protection and consideration by the courts. When these values come into conflict, as they often do, it is necessary for the courts to make choices based not upon an abstract, platonic analysis, but upon a concrete weighing of the relative significance of each of the relevant values in our community...*

This case involved sexual assault and interference charges relating to young females. On a motion by the crown, consented to by defence counsel, the trial judge ordered the exclusion of the public and the media from parts of the sentencing proceedings dealing with the specific acts committed by the accused, pursuant to s. 486(1) of the Criminal Code. This was due to the "very delicate" nature of the evidence. The trial judge stated that he made the exclusion order in the interests of the "proper administration of justice" to avoid "undue hardship on the persons involved, both the victims and the accused". The CBC challenged the constitutionality of s. 486(1) before the Court of Queen's Bench. The Court held that s. 486(1) constituted an infringement on the freedom of the press protected by s. 2(b) of the Canadian Charter of Rights and Freedoms but that the infringement was justifiable under s. 1 of the Charter. The Court also held that the trial judge had not exceeded her jurisdiction in making the exclusion order. The Court of Appeal affirmed the judgment.

5.4 Independence : A Unique, Cornerstone Value within Courts

One of the most unique and fundamental values within the core value set proposed by the Consortium for Court Excellence is *independence*.

Within Canadian jurisprudence, a relevant description was articulated by Le Dain J in *Valente v. The Queen*, [1985] 2 SCR 673 at para 20:

> *" It is generally agreed that judicial independence involves both individual and institutional relationships: the individual independence of a judge, as reflected in such matters as security of tenure, and the institutional independence of the court or tribunal over which he or she presides, as reflected in its institutional or administrative relationships to the executive and legislative branches of government.*
>
> *…. The relationship between these two aspects of judicial independence is that an individual judge may enjoy the essential conditions of judicial independence but if the court or tribunal over which he or she presides is not independent of the other branches of government, in what is essential to its function, he or she cannot be said to be an independent tribunal."*

The closely related 'Separation of Powers' principle was defined in *The Queen v. Beauregard*, [1986] 2 SCR 56 at para 30 per Dickson CJ as follows:

> *"The role of the courts as resolver of disputes, interpreter of the law and defender of the Constitution requires that they be completely separate in authority and function from all other participants in the justice system."*

It was also discussed by McLachlin J in *New Brunswick Broadcasting Co. v. Nova Scotia (Speaker of the House of Assembly)*, [1993] 1 SCR 319 at page 389 as follows:

> *"Our democratic government consists of several branches: the Crown, as represented by the Governor General and the provincial counterparts of that office; the legislative body; the executive; and the courts. It is fundamental to the working of government as a whole that all these parts play their proper role. It is equally fundamental that no one of them overstep its bounds, that each show proper deference for the legitimate sphere of activity of the other."*

In the *United Nurses of Alberta v. the Alberta Attorney-General* (1992) 1 SCR 901 at 931:

> *"The rule of law cannot exist without an independent judiciary to uphold its authority. It is directly dependent on the ability of the courts to enforce their process and maintain their dignity and respect"*

Those involved in information management policy formulation, and court information system design, need to fully appreciate the values that are unique to the court environment, such as *independence*, alongside other values considered to be fundamental to the effective operation of courts.

6 WHAT IS ARCHITECTURE?

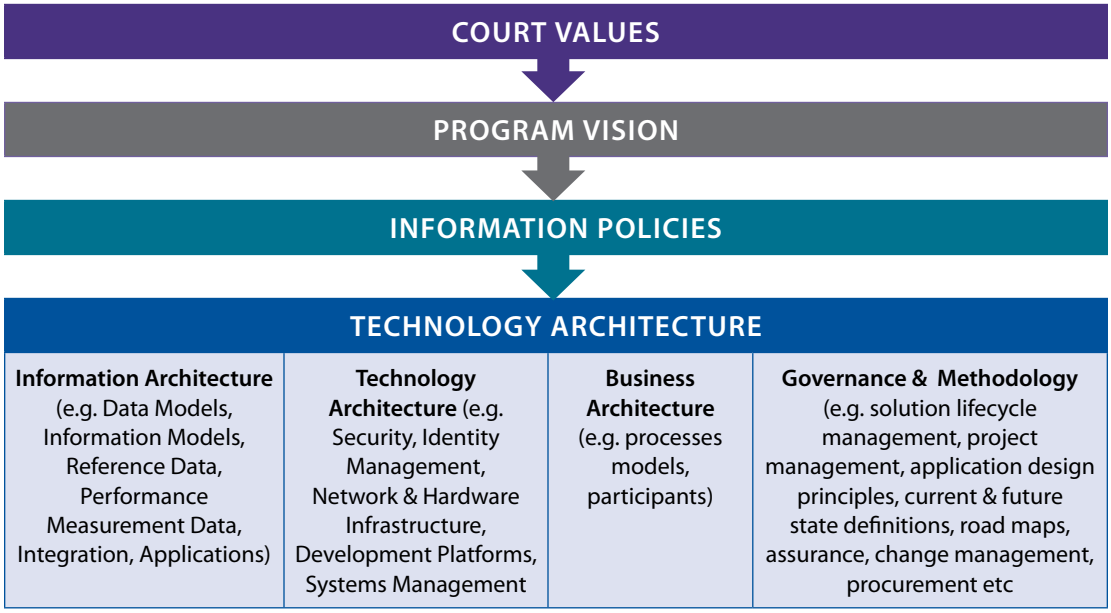
The term "IT architecture" means different things to different people. In the business technology domain it is generally understood to mean the enabling "framework" that will support the business as it evolves towards the desired future state as articulated in a Vision statement. This "future state" often involves business transformation supported by technology.

A more specific definition of architecture is:

"A set of principles, guidelines, policies, models, standards, and processes and the relationships between these artefacts that guide the selection, creation, and implementation of solutions aligned with business goals"[17]

In essence, architecture is a framework that supports and guides decision making in relation to technology solutions. The following diagram shows the key elements of the IT Architecture within the context of the Values hierarchy model presented earlier in this document.

Diagram 2: Inter-relationships between Values, Policies and Architecture



[17] US Department of Justice's Global Justice Reference Architecture Specification version 1.7, March 2009, Glossary Definition at line 1074

The key elements; Information Architecture, Technology Architecture, Business Architecture and a Governance and Methodology Framework are described below.

Information Architecture

The information architecture identifies the information that needs to be managed and the inter-relationships within this information. It is advantageous to draw upon a set of policies that articulate agreed definitions for the vocabulary and unique terms used within the organisation. Policies such as these are often contained within a glossary of key terms defined by senior executives or policy makers. Information models need to be translated into data models for implementation within computer systems.

Important information is often implemented as reference data, or look up "codes" that must be recorded consistently to deliver information integrity, reliability and accuracy. This core business data is often exchanged between multiple agencies and systems and to produce statistical reports so consistent terminology is of paramount importance. Some common examples of reference data in the justice arena include "offence codes", "court order codes", "sentence types", "hearing categories", "legal representation types", "document types", and "cause of action types".

Performance measurement data is usually defined within the information architecture via documented data definitions and counting rules used to consistently record operational performance, workload levels and other trends. Statistical reports containing such metrics can be used for benchmarking or to support management decision making and policy development. Some examples of reporting metrics that are commonly used in the court arena include "backlog", "workload", and "clearance rate".

Technology Architecture

The technology architecture incorporates the preferred, mandated and supported hardware, software application, development and operating system platforms. This is often encapsulated in the documented Standard Operating Environment ("SOE"). It also identifies current network, security and hardware infrastructure, hosting arrangements and communication protocols.

More recently, identity management components, standards and protocols have also been incorporated within the technology architecture.

Business Architecture

Business process models represent in a consistent, industry standard notation the flow and interaction between user activity and system functions when performing common business tasks. These may be expressed in current terms ("As-Is") or in future terms ("To-Be") to reflect desired future state process improvement opportunities.

Governance & Methodology

A governance framework is required to manage and evolve the Information Technology Architecture to ensure it is implemented effectively in practice and that it remains aligned with business objectives, strategies and policies.

The Solution Development Lifecycle Management methodology is a documented approach to the initiation, development, procurement, implementation, integration, migration and retirement of new technology solutions. This methodology usually includes change management components

and an assurance model that provides gateway reviews by a steering group to ensure progress is in line with project objectives and plans and remains aligned with broader architectural and policy mandates.

A Project Management Methodology is a documented, industry recognised methodology to support opportunity assessment, initiation, planning, management and delivery of projects. All projects pursued within a program of work should be managed consistently in accordance with the program's endorsed methodology. The methodology should incorporate gateway reviews or "health checks" before moving to the next stage and directives and templates relating to the initiation, planning, management and delivery of projects.

It is common to articulate preferred software application design principles (e.g. Service Oriented Architecture, Client Server Architecture, Thin Client Architecture etc) to guide the way software is developed and to direct the evaluation of Commercial Off The Shelf ("COTS") solutions. There is an increasing international trend towards the use of *Service Oriented Architecture* due to the agility it delivers.

6.1 Why do we need Architecture?

Architecture helps to align diverse technology and business improvement projects, to direct them towards a common long term Vision and align them with broader information management policies.

It provides a baseline against which all proposed project activity can be checked to ensure that new technology will be as compatible, consistent and interoperable as possible and to ensure that system functionality and information capture is not duplicative across an organization.

Alignment of projects within a broader architectural foundation enables system support and maintenance costs to be minimized and staff training needs to be simplified through the use of common and consistent application interfaces and technology platforms. It maximizes opportunity for re-use of functionality by different business units across the organization or by external clients and stakeholders.

When embarking upon the redesign and automation of a particular business activity it is important to address the immediate operational needs at hand but it is also important to have one eye on the bigger picture. Architecture provides this 'top down' perspective.

6.2 What is the risk of proceeding without it?

It is possible to build new systems in an organic manner without a master plan however it's risky. There is a danger that immediate business needs may be addressed by separate and distinct technology solutions that may evolve piecemeal over time without any consideration or appreciation of longer term objectives and opportunities. What can eventuate is a complex mesh of technologies that do not interrelate, are expensive to maintain and are too rigid to adapt to changing needs.

This means that opportunities to leverage prior investments in technology may be reduced and the potential to eliminate duplication and share information across multiple systems and organizations may be compromised. Short term gain may deliver long term pain if architectural considerations are not squarely placed on the agenda for all new project proposals and at critical checkpoints throughout the development life cycle of a project.

The following quote is an extract from an email sent by a CIO within a Commonwealth Department of Justice. The purpose of the email was to explain why he intended to engage an architect to review the technology environment within the department.

> *"I've inherited a bunch of technology and business applications that together look like a pre-fabricated hen house. It's a hodge podge of disparate applications based on diverse, incompatible technology platforms.*
>
> *This inconsistency means there's little opportunity to effectively share information across systems even within the organization let alone with external stakeholders and there's limited scope to leverage prior IT investments. It is also virtually impossible to consolidate support and maintenance arrangements to improve efficiency and effectiveness or to adapt quickly to meet changing strategic directives.*
>
> *Many staff are faced with the need to log on to multiple software applications in any given day, each with a different interface, and to re-enter the same information multiple times in these separate, systems. Loss of faith in the central systems has also led to the creation of hundreds of spreadsheets across the organization which further entrenches data integrity, reliability and redundancy problems... "*

This is what happens when there is no architectural foundation and little planning around new system developments.

Before architects can effectively roll up their sleeves there needs to be an articulated project or program Vision and a set of core Values reflected through endorsed and well documented information management policies. These policies effectively operate as Architectural Principles to guide the design of the technology solutions.

6.3 Emerging Trends : Service Oriented Architecture

Traditional architectural approaches to system design and implementation are restrictive, inflexible and do not easily accommodate our new networked society.

Modern architecture approaches are more in tune with this new paradigm. For example, Service Oriented Architecture ('SOA') may potentially deliver the 'best of both worlds' in so far as it can deliver control and autonomy over information to custodians without compromising information exchange, access, interoperability and adaptability.

Indeed, there is no need for any system to be an island in this new networked world. It is quite possible, to design an architecture that delivers autonomy and control for information custodians in the courts, while concurrently servicing other obligations such as access arrangements and information exchange with other government agencies.

There is considerable work underway in many international jurisdictions to embrace service oriented architecture within the justice domain due to the fact that it presents a solution where interoperability is required without compromising software application independence in specific business areas. This also represents best practice for large scale computer system design and development.

A service-oriented architecture is essentially a collection of services that interact with each other though simple data transfers. Services may interact over a network or, in the case of "web services", over the Internet or in 'the cloud'.

Benefits of Service Oriented Architecture

Service Oriented Architecture ("SOA") is said to deliver faster application development and applications that easily adapt to meet changing needs.

SOA enables autonomous services to be loosely assembled into service-oriented applications that can be as cohesive externally as applications built with traditional approaches. The terms 'loosely coupled' and 'coarse grained' refer to the fact that the services are gathered together but are autonomous in so far as the only exchange or interface between them is in terms of pre-defined messages. This delivers interoperability without compromising the need for software application independence.

The benefit of SOA over more traditional 'tightly coupled' integration approaches is that SOA-built systems enjoy increased agility, greater tolerance for change, flexibility and modularity.

Basically, when this approach is adopted, it is possible to modify one web service substantially without affecting another service that calls it and vice versa as long as the pre-defined message structure between the two services does not change.

This architecture is also well suited for applications that involve synchronous communication over distributed networks such as the Internet.

Service Oriented Architecture is particularly relevant when it is important to maintain independence and flexibility within various discrete functional business areas across enterprise wide solutions or where it is necessary to interconnect separate independent systems for information exchange.

A SOA message oriented architecture will also support flexible interactions between organisations using a simple, bulk data exchange. This can be achieved, for example, between court systems and large consumers of court services such as government agencies.

Migration from legacy applications into new technologies

SOA can also provide a manageable, low risk pathway to enable phased retirement and migration away from large scale, entrenched, obsolete technology onto contemporary network enabled applications. This is achieved through migration of business logic into new front end technologies that interact via 'loosely coupled' messages with legacy back end databases.

Service Oriented Architecture in Practice

A Service Oriented Architecture has been embraced, for example, by the Federal Court of Australia within its eCourt strategy that was devised around 2006. The plan involved gradual migration away from a legacy, outmoded case management system ('Casetrack') into a suite of new web based applications that delivered court services in key business areas such as eLodgment, eSearch etc. Casetrack was based on antiquated technology, was cumbersome to use and was shared across three federal jurisdictions; the Family Court, the Federal Court and the Federal Magistrates Court.

Gradually, Casetrack transitioned to become a back end repository for court information rather than an all encompassing front end application for court staff. The 'front end' user interface was, over time, replaced with more contemporaneous web based functionality. This is depicted in diagram on the next page.

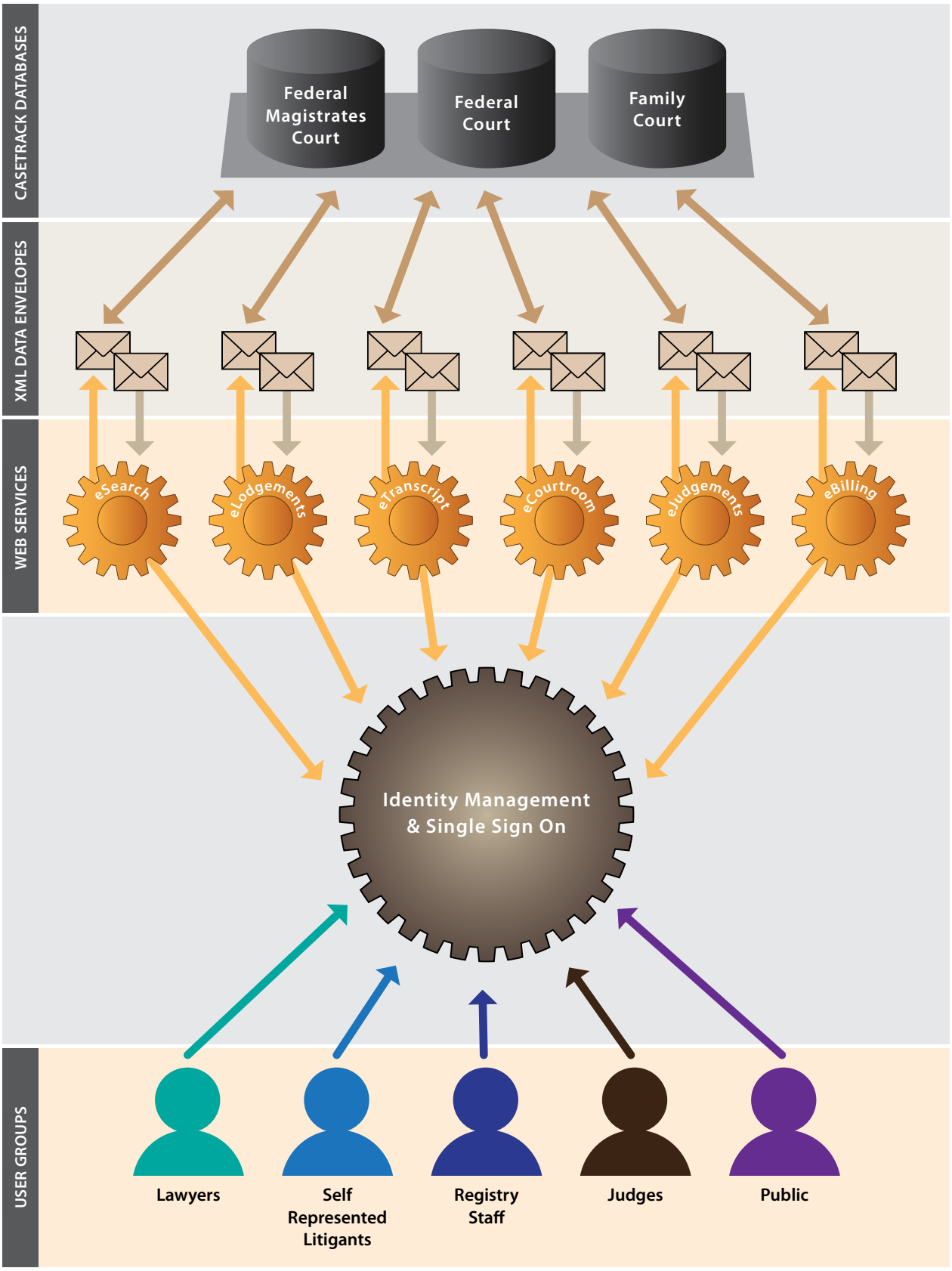
The diagram also shows how different 'services' (or systems) such as eLodgment and eSearch shown in the orange coloured cogs, could be developed independently, even by by different vendors or development teams without compromising either data interoperability or the user experience of an integrated system.

This approach ensures users are presented with a single web browser interface that provides the perception of a single integrated service although behind the scenes, the systems may technically be separate and may even be housed in different locations (e.g. on the court network, in a government intranet, with an Internet service provider or even with a third party provider in 'the cloud').

This approach provides significant flexibility in terms of the possible location of core services and potential integration of pre-existing third party (e.g. 'cloud) offerings. Ultimately, the location and usage of such services becomes a strategic policy decision.

A higher risk and more traditional architecture would have been to develop all the new functionality shown in the orange cogs (eSearch, eLodgment, eTranscript, eCourtroom, eJudgments, eBilling etc) within a single central system and to also transition all the key case management functionality of the legacy system into the centralized replacement system. Such an approach would have involved significant technical risk, complexity and cost and was therefore considered less likely to be successful.

Diagram 3: Federal Court of Australia : Future Case Management Systems based on SOA



This strategy enabled the Federal Court to retain its independence from the business operations of the other jurisdictions even though there was a shared 'back end'. It facilitated the modular, independent development of specific business applications designed to meet particular needs while ensuring that they were able to interoperate.

This architectural approach highlights the importance of information definition and policy formulation due to its intrinsic dependency on message exchange between different 'services'. The technical descriptions (or specifications) of the information exchange packages is not possible without consistent definitions of information components and clear policy guidelines regarding 'access'.

Resources and Capability

Service Oriented Architecture enables large scale automation projects to be delivered in separate and distinct manageable projects that minimise financial and technical risk. Because there is an inherent modular approach involved in building such solutions, program budgets and governance arrangements can be compartmentalised according to defined short to medium term deliverables. These separate and distinct projects should deliver the benefits of independent development without compromising interoperability and information exchange. They should also deliver short to medium term business outcomes and a return on investment while remaining true to the broader architectural blueprint.

The challenge and risk to be mitigated, of course, is; securing and retaining appropriately skilled people with the experience and capability to actually implement such solutions.

7 DEFINING COURT INFORMATION – A GRANULAR PERSPECTIVE

7.1 Why do we need definitions?

As discussed earlier, it is becoming increasingly important to recast traditional policies regarding management of court information to accommodate new opportunities and risks in our digitized and networked world.

While there has been, over recent years, much debate regarding *access* to ***Court Records,*** it is often difficult to ascertain exactly what is meant by the term ***Court Record*** as it has been so loosely and inconsistently defined and has been used in so many different contexts. A clear, contemporaneous and workable definition is urgently required to clarify this uncertainty, to facilitate more focussed debate and to provide guidance for the architects of our future court information systems.

It is apparent that a considerable amount of analysis and debate has been undertaken in relation to the desire for 'transparency' as courts contemplate their on-line presence. There often appears to be a broad assumption that 'transparency', can best be achieved through unfettered ***access*** to ***Court Records*** even though that term is rarely defined in a clear and consistent way.

It appears that this mindset has unfortunately skewed the debate in so far as it is focussed almost exclusively on the need for 'transparency' while, to some extent, other equally important values that underpin an effective justice system including 'public confidence', 'fairness' and 'human dignity" have been sidelined.

It could be argued, for example, that protection of privacy and respect for civil liberty must be given equal weighting by the courts because these are essential principles of a democratic society. An infringement of privacy will often amount to an infringement of liberty. Attention to fundamental human rights including a right to privacy, may strengthen public confidence in a court's ability to handle sensitive information appropriately.

The US Department of Justice's Global Justice Information Sharing Initiative pursues large scale sharing of critical justice information while vigilantly considering the privacy rights of individuals. An articulated priority is :

> *"To protect civil liberties by strengthening privacy protections in the digital age. .. Without safeguarding privacy and civil liberties of our nation's individuals simultaneously and with equal zeal as the pursuit of data exchange capabilities, endeavours in this arena will ultimately fail."* [18]

The extent to which potentially disturbing, private or commercially sensitive information is contained on court records and the inherent risks to both individuals and the community at large that could result from unfettered access to it is often overlooked by open access advocates. This oversight largely relates to the lack of a clear and detailed definition for the term ***Court Record*** and lack of due consideration of the inherent risks of our networked society as canvassed earlier in this document.

Those that advocate broad and open access to ***Court Records*** as a starting position are often referring to loose, ill-defined, generic notions of court information. However, court information management policy needs to be tailored to accommodate not only the diverse range of information that finds its way onto ***Case Files*** but also the considerable differences between, for example, the nature of the information held on criminal cases, on commercial disputes cases and on family law or young offender cases.

It is therefore suggested that focus now needs to shift beyond platitudes associated with '*access*' to court information to address specific policies relating to the management of all court information.

'Access to ***Court Records'*** is only one, albeit an important, policy area that needs to be clearly serviced alongside other equally important policy areas in order to preserve confidence in our legal system.

In order to establish an effective information management policy framework for courts it is necessary to first define the key terminology to be used.

Not only will this facilitate a meeting of minds between the policy makers, it will also enable foundational concepts to be described in language that can be clearly understood by the technologists and architects responsible for design and implementation of justice information systems.

This is particularly important given that architects and technologists that are engaged to work on court automation projects have often had extensive experience in government implementations yet little prior exposure to the justice sector. They may not, therefore, fully appreciate some of its unique characteristics, including, for example, the cornerstone principle of *judicial independence*.

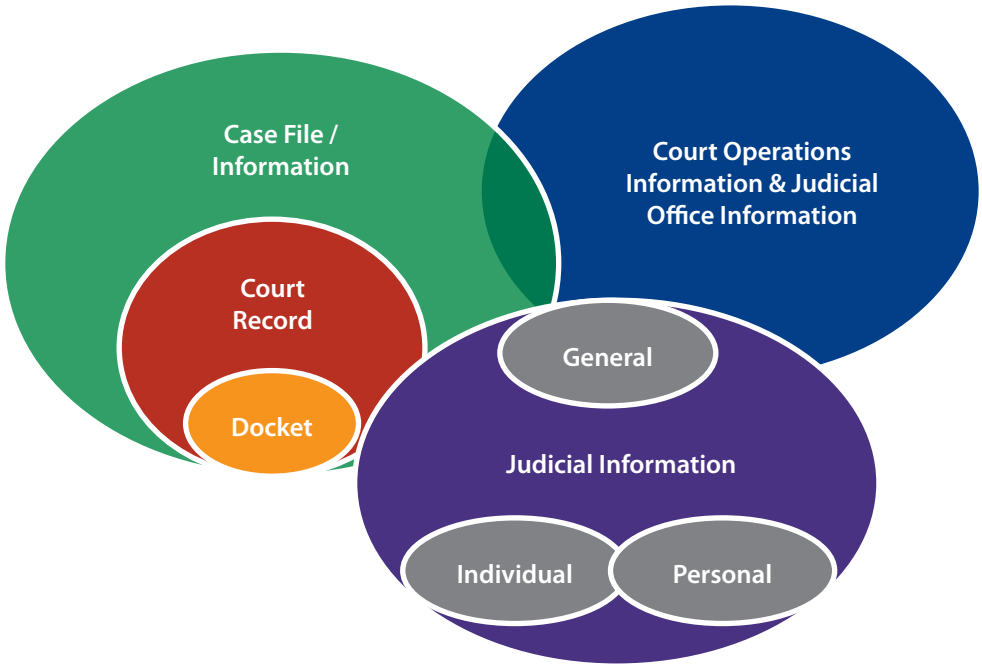
[18] US Department of Justice's Global Justice Information Sharing Initiative, 15 December 2008 – Page 2

7.2 Categories of Court Information

In a modern court environment *documents* are no longer the only mechanism through which information may be captured and exchanged. A large percentage of court information is today held in database fields in software applications rather than in paper documents. It is therefore important that our definitions of court information move away from the traditional document centric perspective. Our definitions must include all information that is managed within courts even if is captured in database fields rather than in traditional 'documents' as is contemplated by most court rules.

The diagram below identifies some of the main terms regularly used in relation to court information and provides a proposed graphical representation of the inter-relationships between these common terms.

Diagram 4: Court Information Terms and Inter-relationships



This diagram shows that a ***Case File*** is one category of court information while a ***Court Record*** is a sub-set of the information contained on a ***Case File***. Some types of ***Judicial Information*** will fall entirely outside the realm of court information altogether while other types of ***Judicial Information*** may also be considered to be court information. Some ***Judicial Information*** may, at the discretion of the judge or through the application of court protocols and procedures, be effectively deposited onto a ***Case File*** or a ***Court Record***.

A simple way to interpret the diagram is to focus first on the ***Court Record*** as the sub-set component of the ***Case File*** that is to be made broadly accessible to the public, subject of course to other policy constraints such as removal of personal identifier information, etc. The ***Court Record*** is also the official record of proceedings that will be preserved indefinitely to capture the history of events that transpired on the case while it was within the realm of the court.

In this context, it is interesting to consider the similar approach embraced by the Court Information Act 2010, No 24 New South Wales, Australia. This an example of the legislature stepping in to clarify access arrangements for court information and to define key terms due to the absence of consistently applied policy across New South Wales courts. In particular the definitions of 'Court Record', 'Open Access Information', 'Restricted Access Information' are an attempt to effectively partition the information residing on case files into those components that should be accessible to the public (our ***Court Record***) and those that should be restricted to the parties (our ***Case File***)

The proposed definitions for the foundational terms shown in the diagram are presented in Appendix 3 and background considerations for these are discussed below. The definitions in Appendix 3 are designed to be *generic* enough to apply across a variety of jurisdictional areas and *medium neutral* in that they can apply equally to digital information and paper documents.

It should be noted that the CJC's Model Access Policy provides some potentially useful definitions of key terms although they may not be specific or granular enough to provide a solid platform for information management policy development outside the realm of 'access policy'.

Judicial Information

The Canadian Judicial Council's Blueprint for the Security of Judicial Information Third Edition 2009[19] provides guidelines and suggested policies relating to security and integrity of computer systems containing 'Judicial Information' and defines the roles and responsibilities of judges and administrators in this context. The Blueprint defines the term as follows :

> *25. "Judicial information" is information gathered, produced or used for judicial purposes, but does not include:*
>
> - *Court Services administrative policies and procedures and information specifically gathered or produced for the purposes of managing those court policies and procedures;*
> - *The chronological listing of court proceedings;*
> - *Exhibits, affidavits and other written evidence filed with the Court;*
> - *Documents, rulings, endorsements, orders, judgments and reasons for judgment that have been issued" (i.e. published).*
>
> *Judicial information is created by judges, including judicial officers such as Masters, Registrars, and Prothonotaries, and judicial staff, including any employees or contractors who work on behalf of judges and whose work includes the handling of judicial information, such as executive officers, law clerks, law students, judicial clerks or assistants and judicial secretaries. Together, judges and judicial staff are referred to as — judicial users.*

[19] http://www.cjc-ccm.gc.ca/cmslib/general/JTAC-ssc-Blueprint-Third-edition-finalE.pdf

This definition hinges on the expression 'for judicial purposes'. This could itself be open to interpretation which could lead to inconsistent application, implementation risks and potential exposure of highly sensitive information.

It is suggested, therefore, that the definition could be recast to clearly establish the fact that the following specific types of information are to be considered ***Judicial Information***:

- Information relating to private or personal affairs and social interactions of a judge
- work relating to a ***Case File*** that is highly sensitive in nature (e.g. draft judgments)
- audit logs containing summaries of computer system activities undertaken by a judge
- history of web sites visited by a judge
- Judicial email correspondence that does not directly relate to a ***Case File***
- All sms and voice mail messages
- diary and calendar events other than docket events that directly relate to a ***Case File***
- contact details including address book information held on mobile phones or in desktop software applications or other electronic repositories
- social networking information that is not in the public domain, for example private blogs or closed collaborative networks used by judges and their professional colleagues
- information regarding the scheduling of judges within a court calendar
- the content used for judicial education programs
- information regarding a particular judge's attendance at educational programs
- statistics showing a judge's individual activity or workload
- personal notes, research or working papers produced by or on behalf of a judge that have not been deposited on a ***Case File***
- judicial committee or board work including communication and research materials
- judicial benchbooks.

Furthermore, it should also be clearly understood by those designing implementing court systems that although the following information categories may be considered ***Judicial Information*** in so far as they are created or used 'for judicial purposes' they might sometimes be incorporated into the ***Case File*** in which case the policies applicable to that category of court information including broader access arrangements should apply rather than the more restrictive rules applicable to ***Judicial Information***-

- Electronic or paper based correspondence between a judge and the parties in relation to the management of a ***Case File*** (for example, emails requesting documents from the parties, suggesting case management timetables, requesting extensions, negotiating hearing dates etc); and
- Draft orders exchanged between the judge and the parties

While such materials are 'used for judicial purposes', and therefore satisfy the Judicial information test, they are invariably included on ***Case Files,*** and in some jurisdictions they are even made generally available to the public (i.e. considered part of the ***Court Record***) before they are in final form. Ultimately, the policy framework presented in this document will support either approach.

Judicial Information that has not been included on the ***Case File*** is highly sensitive information with very tight security and restrictive access arrangements.

However, from time to time, in certain circumstances ***Judicial Information*** may, through exercise of judicial discretion or in accordance with established policy and protocols, evolve to a point where it is incorporated into a ***Case File***. From that point onwards, it will generally be appropriate to manage it as ***Case File*** information. Conversely, there will be some categories of ***Judicial Information*** that never even become court information. Such information may relate, for example to private email communications to, from or between judges that do not relate to court business at all.

A judgment, once signed and filed will generally be incorporated into the ***Court Record*** however, at the earlier draft stage it must be managed as ***Judicial Information*** and must not be intermingled with the ***Case File***. Deliberative secrecy safeguards judicial independence in the decision-making process. Judges cannot be compelled to testify about their decision-making process (See *Duhaime, Mackeigan v. Hickman*, [1989] 2 SCR 79), and for the same reason, information that relates to that process is not accessible to parties or the public.

The proposed definitions relating to ***Judicial Information*** contained in Appendix 3 are an attempt to sub-categorise ***Judicial Information*** to reflect the considerations outlined above.

Case File

The terms 'Case File' and 'Court Record' are often used interchangeably however, in the increasingly electronic landscape the term 'file' can lead to confusion. Technologists will often assume the term refers to an electronic file from a computer system rather than a physical cardboard folder containing paper documents. For this reason, and to avoid confusion, it is important to provide a clear definition of the term.

A ***Case File*** contains the documents and information that directly relate to a single court proceeding or to a number of related court proceedings that have all been assigned the same case file number. It includes the information and documents that comprise the ***Court Record*** and any other documents or information that have been captured or placed on the ***Case File***.

Court Record

This term refers to the "Official" ***Court Record***. It is the portion of the ***Case File*** that will be made accessible to the public, subject to privacy constraints regarding, for example, disclosure of personal information etc. The ***Court Record*** should be preserved indefinitely whereas the rest of the ***Case File*** is usually destroyed after a defined period of time.

The CJC's Model Access Policy defines ***Court Record*** as follows:

> *"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.*

It is suggested that this definition could be recast to avoid confusion and to reflect the proposed inter-relationship represented above in terms of ***Court Records*** residing within ***Case Files***.

Docket

The CJC's Model Access Policy defines Docket as follows (1.3.4):

> *"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.*

This definition is considered to be sufficient for information management policy formulation purposes; however it may be helpful to clarify the fact that the ***Docket*** is a sub-set component of the ***Court Record***.

As an integral part of the ***Court Record***, the ***Docket*** should be subject to the same information management policies regarding access, security, privacy, preservation etc.[20]

7.3 Court Users and Participant Categories

Court users and participants will generally fall into one of the following categories:

Court Participant / User Category	*Details*
Judiciary	Includes Judges, Masters, Justices of the Peace, Registrars, Case Management Officers, Judicial Staff (including Articling Students, Legal Counsel, Judicial Assistants)
Registry	Includes Registry Staff, Sheriffs, etc..
Parties	Includes civil litigants, accused persons, prosecutions, legal representatives, third party (e.g. by election), subpoenaed parties, self represented litigants
Witnesses	Includes persons called upon to give evidence in criminal or civil proceedings.
Jurors	Includes jurors participating in civil or criminal proceedings.
Criminal Justice Agencies	Includes those government agencies and departments involved in the administration of criminal justice including department of justice, correctional institutions, police and law enforcement, family services, prosecutions, legal aid
Other Government Agencies	
Media	
Public	
Victims of Crime	
Educational & Research Organizations	
Authorised Publishers, Distributors & Aggregators	
Unauthorised Publishers, Distributors & Aggregators	
Other Judicial and Court Agencies (other jurisdictions)	

The defined court participant and user categories identified above are used within the table in Appendix 2.

[20] The docket is part of the court record and subject to the same rules of access: *Alberta (Attorney General) v. Krushell*, 2003 ABQB 252.

7.4 Case Type Categories

A Court Information Access Grid will be prepared for each Case Type including:

- Criminal
- Civil
- Family
- Youth
- Probate
- Corporations
- Bankruptcy
- Personal Injury
- Etc …

7.5 Personal Information

The CJC's Model Access Policy (1.3.7) defines Personal Data Identifiers as follows:

> *"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).*

Note the exclusion of name and year of birth. For the purposes of this policy framework this definition may be too narrow due to the requirement that the information will only be classified as 'personal data identifier' if its disclosure will actually pose a serious threat to an individual's personal security. This is quite a restrictive test which may, as a result, lead to unnecessary disclosure of sensitive, private information.[21]

A proposed alternative definition is included in Appendix 3.

---

[21] By comparison, the Court Information Act 2010, No 24 New South Wales, Australia applies a broader and perhaps more practical definition of Personal Identification Information as follows:
"personal identification information" means any of the following information concerning a person:
(a) tax file number,
(b) social security number,
(c) medicare number,
(d) financial account numbers,
(e) passport number,
(f) personal telephone number,
(g) date of birth (other than year of birth),
(h) home address (other than suburb, city and State or Territory),
(i) other information that can be used to establish a person's identity
and that is prescribed by the regulations as personal identification information for the purposes of this Act.

8 COURT INFORMATION MANAGEMENT POLICIES

8.1 Policy Formulation

There are a number of areas of court information management policy that require development or rejuvenation to accommodate the unique characteristics of electronic information and the emerging risks within a digitized and networked society.

Well articulated court values provide a foundation for this policy development. However, the subtle nuances and potentially competing aspects of these values require detailed consideration, analysis and debate. Trade-offs will often be necessary as this balancing act is undertaken. For example, it may be necessary to compromise access arrangements in certain circumstances to protect the safety of participants involved in court proceedings or in the broader interests of justice.

Information Management policy development can be a challenging exercise involving complex consideration of what may, at times, appear to be conflicting rights and interests. For this reason, it is important that it is undertaken, or at least endorsed, by an engaged judicial leadership group. Where this does not happen, the architects responsible for the design of court information management systems may make dangerous decisions based on incorrect assumptions.

The recommended court information management policy framework presented below is divided into the following subject areas:

- Foundational Policies
- Access Policies
- Privacy Policies
- Security Policies
- Preservation Policies
- Performance Measurement Policies

Each policy area is represented in tabular format to clearly show the policies falling within it, the underlying rationale and the broader court values they augment.

The definitions articulated earlier in this report provide the building blocks for information management policy development. Where defined terms are used, such as ***Court Record***, ***Case File*** etc., these are represented in italics with a bold font.

8.2 Foundational Policies

The foundational policies apply across the board and provide a platform for policy formulation in each of the other specific subject areas. They also position courts to embrace many of the operational and service delivery benefits that can be derived from effective implementation of information management systems.

Foundational Policies

Policy	*Rationale*	*Court Values Enhanced by Policy*
1. Key terminology will be defined for consistent application across all courts and subject areas	• To document and effectively communicate information management policies, frequently occurring and foundational terminology must be clearly defined, well understood, and used consistently. The glossary contained in the Appendix provides a first-draft attempt to formulate such definitions. • 'Case File', 'Court Record', 'Court Docket' and 'Judicial Information' are properly defined first. • Further commonly-used terms that benefit from clear and consistent definitions include 'case', 'matter', 'proceeding', 'party', 'litigant'. • Performance-related information elements include 'backlog', 'clearance rate', 'finalization' • 'Personal Information' must be clearly defined because this category of court information will involve specific access arrangements to protect privacy.	Transparency, Public Confidence, Effectiveness
2. Ultimately, the official Court Record and the Case File will be in electronic format.	• Information now delivered to the courts in paper form was initially created electronically. • Information is increasingly being delivered to courts in electronic form, via eLodgment systems, email, electronic trial or appeal books. • Most information generated by courts is now also created and stored in electronic form by court systems • It is inefficient to convert large volumes of electronic information into paper format purely to produce the 'official court record' • Most courts already have a document management system to provide a repository for electronic documents or intend to establish one in the near future • An electronic court record doesn't necessarily mean a paperless court. Rather, it creates an efficient environment within which ***paper can be produced on demand only when it is needed in that format.*** • This policy leads to dramatic efficiencies when online services are implemented, because it reduces the need for electronic material that is filed with or generated by the court to be later printed by registry officers solely to capture it for inclusion in the paper-based court record. • For these reasons, courts all over the world are contemplating an official electronic record.[22]	Efficiency

[22] According to a 2009 National Centre for State Courts Survey there were at the time 15 US State Court jurisdictions that had established the official court record in electronic rather than paper format. The Federal Court of Australia has also endorsed this strategic objective as part of its document management and 'eCourt' vision.

Foundational Policies

Policy	*Rationale*	*Court Values Enhanced by Policy*
3. Each court needs to determine what information comprises the ***Case File***, ***Court Record***, ***Court Docket, Court Administration Record,*** and ***Judicial Information***	• The distinctions are important as they will determine both access privileges for court users and participants, and preservation obligations. • The system should be designed to be capable of such recognitions and distinctions on an automatic basis. • This analysis should be undertaken for each ***Case Type*** using the table contained in Appendix 2 • The analysis should incorporate the Fair Information Principles (e.g. minimal collection).	Access, Transparency, Effectiveness
4. Court information systems and technologies should be procured, designed and implemented in a manner that facilitates interoperability and data exchange between different systems, all without compromising systems independence, judicial independence and the Courts' role as custodian of Court Records.	• Best practice will be adopted by solution architects when designing and implementing court information systems . At this point in time, a Service Oriented Architecture ("SOA") is the desirable approach and represents best practice. • The system design should permit transfer and sharing of input data subject to proper screening, confidence and security measures between the systems.	
5. Wherever possible data should be entered once only, at the source	• Duplicated data entry leads to inefficiency and is highly error prone. • All court information has an original source and this is where it should be captured. Some of this information has an origin outside the court, for example in a police department where criminal charges are first entered, or within the offices of law firms where lawyers responsible for the case prepare documents to initiate new court proceedings. • Justice information system designs should accommodate these original information capture points and thereafter it should be possible to electronically exchange information rather than re-enter it repeatedly as a file winds its way through the justice system. • An overall system with independence but interoperability, such as the service oriented architecture format, is desirable. The design of the system should permit transfer and sharing of input data subject to proper screening, confidence and security measures as between different systems.	Efficiency, Public Confidence, Quality

Foundational Policies

Policy	*Rationale*	*Court Values Enhanced by Policy*
6. A single personal identifier code should be used wherever possible across all justice agencies and the courts for all persons charged with criminal offences.	• Subject to the need to conduct a Privacy Impact Assessment (refer privacy policies below) when implementing integrated justice systems that involve courts, Single Person Identifier codes should be used for persons accused of criminal offences. • Without Single Person Identifier codes, it is virtually impossible to verify identity and to monitor an accused person through the legal system from charge, to committal to prosecutions, to directions hearings, to trial and potentially on to correctional centers. Names are an insufficient method of identification due to the significant potential for multiple people to have the same name. • These codes must not be visible outside the internal computer systems and automated data-exchange facilities used by agencies and courts involved in the justice sector. • Entity identifier codes may later be considered for the civil justice system; for corporate parties, this could simply be the corporate registry number. • The extent to which single person identifiers should be used for other parties and witnesses, for example, for those involved in family and child welfare matters is a matter for each jurisdiction to determine.	Efficiency, Fairness, Public Confidence,
7. Courts should develop policies that will ensure that technology does not compromise trial fairness or the administration of justice, while permitting parties and their representatives to take appropriate advantage of technology in proceedings and in court.	• Information flow in and out of the courtroom must not compromise trial fairness and the administration of justice. • A court may prohibit the use of cameras and other means of recording or transmitting information, including, without limitation, blogs, texts and tweets. • Jurors should be directed at the start of trials not to perform any independent research, including Internet searches of any of the people or places or issues involved in the case. Nor should they publish any comments regarding the case, including the use of Internet or smartphone services such as sms, mms, Twitter, Facebook, or blogs. • Any person who breaches these directions may be cited in contempt of court and where appropriate, prosecuted for obstruction of justice.	Fairness, Public Confidence
8. All judiciary, court staff, and court communications will use a common Internet domain that is distinct from the government domain.	• The judicial branch of government is separate from the executive and legislative branches. • Public perception should be supported to align with the truth that courts are impartial adjudicators • Judicial and court websites, email addresses and communications must be clearly identified and branded as belonging to the judicial branch. • This is particularly important where a citizen is involved in a dispute with a government agency or in criminal proceedings involving a law enforcement entity that uses a .gov domain extension.	Independence, Transparency, Public Confidence, Fairness, Efficiency

Foundational Policies

Policy	*Rationale*	*Court Values Enhanced by Policy*
9. Email usage protocols will be developed and published to guide judges, court staff and external court users and participants.	Each jurisdiction should consider the extent to which the following policies should be adopted: • Anyone filing a document with the court must provide an email address. • Email will be encouraged as a preferred mode of communication with the court rather than traditional modes such as transmission of paper based correspondence through the post or via facsimile transmission. Each jurisdiction will develop email protocols to address: • Circumstances appropriate for email communication • Protocols for copying the parties, the court, including how to address the court (judge's chambers, registry officer, central mail box clearing house etc) • preferred format for attachments (PDF, MS Word etc) • Technique used to identify case number to which an email relates (e.g. in the subject field e.g. 'Re 1076/2010 ') • How to capture of email documents for the electronic Case File. • Procedures to deal with improper and unsolicited communications.	
10. Consistency, accuracy and promptness of Court Information and Judicial Information is an essential goal of the system.	• The system will foster real time accurate production of all forms of court records, including transcripts, judgments, orders, directions, certificates, authorizations, fiats and warrants. • As much as possible, formats and contents will be consistent and comply with recognized standards and best practices. • This will facilitate efficient and effective publication via justice systems and online research databases. • It will also facilitate automated management of transcripts and judgments so that they can be cost effectively and reliably integrated into commercial, third party software applications designed for the legal industry.	Effectiveness, Access, Efficiency
11. Cost regimes must ensure that efficient technologies are used and the benefits and costs savings passed along to litigants.	• Regular review of Scale of Costs to ensure that new opportunities for legal representatives to use technology to improve efficiency are accommodated and encouraged. • For example, the allowable rate for printing electronic evidence should be curtailed to reflect cost-effective outcomes. • Duplication of recordkeeping should be avoided.	Access, Efficiency

Foundational Policies

Policy	*Rationale*	*Court Values Enhanced by Policy*
12. A court controlled governance model will be established to manage the Court Information Management Policies. The judiciary will appoint a governance body to develop and regularly review the Policies	• The governance model will operate under the guidance and control of the chiefs of court • The governance model will establish a governance body (e.g. a "Court Information Management Board") with oversight responsibility for the development, communication, implementation and review of the Information Management policies. • The Court Information Management Board will comprise and be driven by experienced judicial representatives • The Court Information Management Board will establish arrangements (for example, through the establishment of an Information Steward, see below) to ensure that Court Information Management policies : - keep up with advances in technology - continue to meet the court's evolving needs - remain aligned with broader Court Values - are adopted and reflected throughout court operations - are implemented in court technology systems - are communicated, applied and enforced. "Once access policies are established, there must be systems in place for communicating, applying and enforcing those policies"[23]	Public Confidence, Transparency, Efficiency, Integrity, Accessibility
13. A 'Court Information Steward' should be appointed to take responsibility for the quality of court information in terms of its reliability, currency, and accuracy.	Each jurisdiction should consider the appointment of a Court Information Steward. • The Information Steward must ensure that policies are consistently and properly applied across court operations. • The steward must also be responsible for the quality, timeliness, and distribution arrangements associated with court information and would provide a linkage between the day-to-day policy implementation and the governance body. • The steward must be given the technological capacity and resources to audit all uses of the system and to initiate investigations of actual or apparent misuses of the system. • The steward may make proposals regarding policy development and revision through the governance structure. • Key staff within operations will also be responsible for auditing functions • Training, coaching and mentoring will be overseen by the Information Steward in relation to the capture of Court Information into court information systems and the importance of data integrity for staff engaged to perform these functions.	Confidence

[23] Austin, Lisa M. and Pelletier F., Synthesis of the Comments on Judges Technology Advisory Committee's Discussion Paper on Open Courts, Electronic Access to Court Records and Privacy, Canadian Judicial Council, January 2005, page 25

Foundational Policies

Policy	*Rationale*	*Court Values Enhanced by Policy*
14. An Information Management Policy Assessment ('IMPA') will be undertaken at the design and implementation stages of any new court information system and at regular intervals during its use.	• It is better to design information management systems up front to be consistent with the policy framework than to incur expense and inconvenience of retrofitting costly mistakes later • The IMPA will ensure that the proposed design complies with the endorsed Information Management Policies • An IMPA should incorporate a Privacy Impact Assessment • The IMPA and PIA will be supervised by the 'Court Information Steward'	Access, Transparency, Effectiveness, Efficiency
15. Consistent Transcript Format and Publication Standards will be embraced wherever possible	• This will facilitate efficient and effective publication via justice systems and on-line research databases. • It will also facilitate automated management of transcripts so that they can be cost effectively and reliably integrated into commercial, third party software applications designed for the legal industry.	Effectiveness, Access, Efficiency
16. Consistent Judgment Format and Publication Standards will be embraced wherever possible	• This will facilitate efficient and effective publication via justice systems and on-line research databases. • It will also facilitate automated management of judgments so that they can be cost effectively and reliably integrated into commercial, third party software applications designed for the legal industry.	Effectiveness, Access, Efficiency

8.3 Access Policies

A cornerstone question for the judicial policy makers in every court is; *Who* should have access to *What* court information and *How* can they use it?

Access policies need to define:

- 'Who' can have access (by reference to the defined categories of ***Court Participants and Users***)
- 'What' they may access (by reference to the defined categories of court information (***Court Record, Case File***) and to the ***Case Types*** (e.g. criminal, civil etc)
- 'How' they may use it including, for example, the ability to create, read, update, distribute, repackage.

In 2005 the Judges Technology Advisory Committee of the Canadian Judicial Council released the Model Policy for Access to Court Records in Canada ("The CJC's Model Access Policy"). The purpose of this policy is to define the guiding principles for access to court records to ensure consistency with statutory and common law rules and to provide guidance for the judiciary in terms of the exercise of their supervisory and protective power over court records.

The CJC's Model Access Policy defines access as "the ability to view and obtain a copy of a court record".[24] It is suggested that this definition is too restrictive as it does not accommodate other types of 'access' such as the ability to create, update, aggregate, distribute and repackage court information. It is also expressly only applicable to ***Court Records*** which is itself a definition that may need some clarification.

The CJC's Model Access Policy supports openness and preserves the notion that all court records should be made available to the public at the courthouse. It also supports the availability of public remote access to judgements and most docket information. Remote access to other court records by the general public is not supported however.

Court users requiring remote access may execute an access agreement with the court. The CJC's Model Access Policy also covers access issues regarding creation, storage and destruction of court records. It strives to achieve a balance between the principle of open courts and privacy and security considerations.

The purpose of the The CJC's Model Access Policy is to provide courts with a framework to assist with the navigation of unique concerns and sensitive matters brought about by new technology.

The policy acknowledges that while technology enables improved access to ***court records***, it also provides a means for unprecedented access to court information which in turn potentially undermines the "practical obscurity" of the already available paper-based court records. The model policy offers an alternative method for court access that aims to preserve "practical obscurity" while maintaining court openness.

The CJC envisioned that the policy would be used as a base on which to build court access policies in Canadian jurisdictions. The policy states[25]:

"(Access) 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.

---

[24] CJC Model Access Policy defines "Access" as the ability to view and to obtain a copy of a court record. (see 1.3.1)

[25] The CJC's Model Policy for Access to Court Records in Canada (2005) – Executive Summary Page ii

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

a. 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;

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

c. 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.

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."

In Vancouver Sun (Re) 2004 SCC 43, the Supreme Court of Canada referred to the open courts principle and held that the Dagenais/Mentuck test (now enshrined within the CJC's Model Policy) provides an adaptable test through which to balance freedom of expression and other important rights such as the right to a fair trial, the right to privacy and the need to protect security.

8.4 The Bellis Proposals : a Modern Framework of Public Access to Court Records

In a 2009 article, Judith Bellis[26], a highly regarded Canadian lawyer with extensive experience in the formulation of public policy, provides an overview and comparative analysis of current legal principles, policies and practices governing public access to court records, including electronic records, in Australia, New Zealand, England, the United States and Canada. It canvasses a wide range of reform proposals that have been made in a number of these jurisdictions in the last decade to ensure the appropriate balance between the public interests in open courts and individual rights to privacy. It offers a recommended framework for reform that could be considered at all levels of Commonwealth and State courts in Australia.

[26] Judith Bellis is General Counsel and Director, Judicial Affairs, Courts and Tribunal Policy, within the Department of Justice Canada.

8.5 Possible Use of Creative Commons Licence

It may be worthwhile investigating the possible use of a creative commons[27] licence to assist with the practical application of the access policies presented below in so far as they relate to mining, re-distribution and re-packaging of ***Court Information***.

8.6 Proposed Access Policies

The proposed access policies are summarised in the table below.

Access Policies

Policy	*Rationale*	*Court Values Enhanced by Policy*
1. Court Fees should not impede access to court information.	• It should be possible to apply for a waiver of fees to accommodate financial hardship. (see CJC Model Access Policy 4.2)	Transparency, Fairness, Accessibility
2. The public are entitled to know that a ***Case File*** exists even where its contents are sealed or subject to a non-publication order	• See CJC Model Access Policy 4.3	Transparency, Accessibility, Public Confidence
3. Terms of Access to court information will be described within a Use of Court Information Matrix (see Appendix 2)	• The matrix in Appendix 2 shows the type of access (Create, Read, Update, Distribute, Repackage) available to each category of ***Court Participant and User*** in relation to categories of court information (***Court Record, Case File, Judicial Information***) • This Matrix should be prepared for every ***Case Type*** within the jurisdiction.	Transparency, Accessibility, Public Confidence
4. Disadvantaged people will be accommodated as far as possible in terms of access to ***court information***.	• Self Represented Litigants ("SRL's") will have access to specialist services (e.g. through specialist court staff, Non-Government Organizations, Community Law Offices or Pro-Bono Lawyers) to ensure they are not disadvantaged through lack of access to ***Court Information*** and services that are increasingly delivered through the Internet • Translation services will be available if required for witnesses or parties • Web site layout, design and behavior will be implemented to best address the individual needs of people across a range of disabilities and age groups. To this end reasonable endeavors will be made to comply with the W3C Web Content Accessibility Guidelines 2.0.	Human Dignity, Fairness, Accessibility, Public Confidence

[27] *see http://creativecommons.org/*

Access Policies

Policy	*Rationale*	*Court Values Enhanced by Policy*
5. Bulk Access to a portion of or the entire Court Record shall be governed by written agreement with the court addressing key issues and risks.	• (Per 5.3 in the current CJC Model Access Policy) 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 and should contain terms and conditions establishing that: a) regular data integrity checks are undertaken to confirm accuracy timeliness and currency, 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, and pardon legislation as well as any other applicable law. c) privacy policies will be adhered to in relation to any re-distributed court information	Transparency, Accessibility, Public Confidence
6. The purpose for which bulk access is sought is crucial to a decision whether to afford access to court information[28]	• It is generally considered that providing access to enable commercial publishers or information aggregators to repackage or sell court information is only remotely connected to the principle of open courts and should therefore not be readily accommodated unless a compelling justification can be put forward.	Public Confidence,
7. Information Management Policies will be published on the Court web site	• Public access to these policies themselves will ensure transparency	Transparency, Public Confidence
8. Information Exchange Protocols will be defined and negotiated with government agencies before court systems are designed and implemented. These protocols will be developed in line with the Fair Information Principles.	• These policies define which information should be exchanged between government and other external agencies or between the courts and high volume users, the frequency with which it should be exchanged and other terms of use arrangements. E.g. terms surrounding the implementation of structured data feeds into or from court information systems. • A starting point for policy formulation in this area is to consider what information is held on ***Case Files*** that is sourced from external agencies? For example: - Criminal History - Police reports - Medical reports - Victim impact assessments etc - Lower court judgments and secondly, identification of the information from ***Case Files*** that needs to be distributed to others on a regular basis. For example: - orders - judgments	Efficiency, Transparency, Public Confidence, Fairness, Accessibility, Dignity

[28] Austin, Lisa M. and Pelletier F., Synthesis of the Comments on Judges Technology Advisory Committee's Discussion Paper on Open Courts, Electronic Access to Court Records and Privacy, Canadian Judicial Council, January 2005, page 25

Access Policies

Policy	*Rationale*	*Court Values Enhanced by Policy*
9. Requests for extended access will be determined by the court in accordance with defined criteria.	• This Policy is derived from 5.1 of the CJC Model Access Policy • Any member of the public may make a request for access to court information 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.	Fairness, Public Confidence, Accessibility
10. Prior to formal acceptance by the court or admission into evidence documents that have merely been 'received' by the court should not be considered part of the ***Court Record***.	• Documents that are merely submitted or tendered should be retained on the **Case File** and should not be included on the **Court Record** until they are actually admitted into evidence by the court or accepted as 'filed' by the registry. • For example; tendered affidavits and exhibits that have not yet been admitted into evidence and fresh evidence applications that have not yet been considered by an appellate court should be held only on the ***Case File*** and should not be incorporated onto the ***Court Record***. • Given that most civil cases settle before trial, many documents that are submitted to the court are never the subject of any judicial consideration and are simply placed on the ***Case File***. As these documents do not form part of the ***Court Record***, they will not be broadly accessible to the media or the public. If the media or public are interested in obtaining access to such documents however, an application can be made to the court.	Fairness, Public Confidence, Dignity

8.7 Privacy Policies

Privacy policies will often provide guidance as to the circumstances under which Access Policies should be modified to protect personal privacy. However, it's not only the right to privacy that can potentially shift access rights; it's also the potential deleterious effect on the proper exercise of justice that needs to be considered.

An important aspect of privacy policy relates to the terms surrounding de-identification of personal information (e.g. what is to be removed, who is responsible for its removal, when should it be removed etc).

The universally accepted Fair Information Practices (from the OECD Guidelines on the Protection of Privacy)[29] are candidates for Privacy Policy within courts. They are :

1. **Collection Limitation Principle**. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. **Data Quality Principle**. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3. **Purpose Specification Principle**. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. **Use Limitation Principle**. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:
   a) with the consent of the data subject; or
   b) by the authority of law.
5. **Security Safeguards Principle**. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
6. **Openness Principle**. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. **Individual Participation Principle**. An individual should have the right:
   a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
   b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;

[29] see the "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8. **Accountability Principle**. A data controller should be accountable for complying with measures which give effect to the principles stated above.

It is recommended that these principles be embraced within a court privacy policy framework.

Ontario's Information and Privacy Commissioner, Ann Cavoukian, Ph.D. developed the term '*Privacy by Design*' during the 1990's to capture the notion that privacy should be embedded into the early design of an organizations technology solutions and that Fair Information Principles should also, as a matter of policy, be embraced at that early stage.[30] Over and above the moral imperative to respect individual privacy rights, Dr Cavoukian suggests that there are many 'payoffs' for organizations that embrace Privacy by Design, including, in particular, for present purposes:

- improved customer satisfaction
- increased trust
- enhanced reputation and credibility
- improved efficiency (e.g. "building privacy in from the outset avoids costly mistakes that will later require expensive retrofits"[31])

It is interesting to see the alignment of these 'payoffs' with some of the key court values articulated earlier in this document.

Dr Cavoukian's team collaborated with the United States Department of Justice, Office of Justice Programs from 1999-2001 to produce a paper called *Privacy by Design Principles for an Integrated Justice System*[32]. The emerging principles can be applied to an integrated justice system, including the criminal justice process, civil court records, juvenile justice information and probate proceedings. The paper describes shows how technology design can implement policy. It also describes how a technology design architect can implement the Privacy Design Principles.

A key consideration when considering privacy policy is the notion that technology may both invade and protect privacy. Indeed, problems introduced by technology are usually best addressed with technology solutions.

---

[30] See http://www.privacybydesign.ca/

[31] Ann Cavoukian, Ph.D. Privacy by Design http://www.ipc.on.ca/images/Resources/privacybydesign.pdf Page 2

[32] www.ipc.on.ca/index.asp?layid-86&fid1=318 (April 2000)

Privacy Policies

Policy	*Rationale*	*Court Values Enhanced by Policy*
1. Court information systems will be privacy-respectful.		Dignity, Public Confidence, Fairness
2. Court users and participants will, as far as possible, be protected from unnecessary distress, embarrassment, the risk of identity fraud and threats to personal safety through unnecessary disclosure of their personal information.	• *"Access and privacy need not be competing interests. If the fundamental question to be considered in determining access (is) the interests of justice, then access policies should take into account not only the importance of promoting open justice, but the need to avoid injustice or prejudice to individual parties. Disclosure of personal or private information in situations that may create risk, embarrassment or unnecessary distress to parties or witnesses may not advance the interests of justice. It may not encourage parties to be honest and forthright with the court and may discourage litigants from turning to the court to resolve their disputes"*[33] • Members of the public who may become court users need confidence that their personal information will be carefully managed and protected and that it will not be inappropriately disclosed to parties that have no legitimate right to receive it.	Dignity, Public Confidence, Fairness
3. Privacy Impact Assessments will be undertaken at the design stage of court information management systems that involve the potential collection, access, use, or dissemination of personal information.		Dignity, Public Confidence, Fairness, Efficiency
4. As far as possible, individuals and organizations will be able to access and retain control over the use of their personal information that is held by courts.		Dignity, Public Confidence, Fairness, Transparency
5. Court rules, procedures and forms will be reviewed to ensure that unnecessary personal information will not be collected.	• Some courts have already reviewed court forms and procedural rules to remove the requirement for parties to provide unnecessary personal information so that it is not received by the court in the first place.	Fairness, Efficiency, Dignity, Public Confidence

[33] Anne Wallace "Overview of Public Access and Privacy Issues" paper delivered at Queensland University of Technology conference, 6 November 2003 at page 25

Privacy Policies

Policy	*Rationale*	*Court Values Enhanced by Policy*
6. Personal de-identification principles will be applied to published judgments, transcripts and other information that is made publicly accessible	• Personal data identifiers will not be made remotely accessible on any publicly available ***Court Record***. (see by comparison 4.6.2 CJC Model Access Policy) • The CJC's Use of Personal Information in Judgments and Recommended Protocol 2005 should be adopted when writing and publishing judgments	Fairness, Dignity, Public Confidence
7. The Parties are responsible for limiting disclosure of ***Personal Identification Information***	• 2.2 CJC Model Access Policy • 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.	Fairness, Dignity, Public Confidence, Efficiency
8. Non-disclosure of ***Personal Identification Information*** within Judgments and court documents	• 2.3 CJC Model Access Policy 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 Identification Information and limiting its disclosure to what is necessary and relevant for the purposes of the document.	Fairness, Dignity, Public Confidence,
9. ***Personal identification information*** will not be displayed on the publically accessible version of the ***Court Record.***	• Personal Identification Information is defined in the glossary.	Fairness, Dignity, Public Confidence
10. Unnecessary ***Personal Identification Information*** shall not be included within documents filed in court	• Rules that govern the filing of documents in the court record shall prohibit the inclusion of unnecessary ***Personal Identification Information*** and other personal information. Such information shall be included only if and when required for the disposition of the case. (See 2.1 CJC Model Access Policy)	Fairness, Dignity, Public Confidence, Efficiency
11. Non-disclosure during storage	• CJC Model Access Policy 3. • 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.	Fairness, Dignity, Public Confidence

Privacy Policies

Policy	*Rationale*	*Court Values Enhanced by Policy*
12. Non-Disclosure of Accused Date of Birth prior to conviction	• The Date of Birth for persons accused of crimes will not be made available on the ***Court Record*** unless they are convicted of the crime. • This is an exception to the general rule regarding de-identification of court information. • Rationale : protect those with the same name who are innocent to make it clear that they are not the accused person ???	Fairness, Dignity, Public Confidence
13. Vulnerable people will be protected from disclosure of ***Personal Identification Information***	• Personal details of witnesses, jurors, victims of crime and children involved juvenile matters will be captured and retained on the ***Case File*** where necessary but they will not be publically available. • As regards juror privacy issues see paper "Making the Case for Juror Privacy: A New Framework for Court Policies and Procedures by Paula L. Hannaford" [34]	Fairness, Human Dignity, Public Confidence
14. If users of court systems are 'tracked' they will be so advised in advance of their usage	• Some courts have implemented policies to track and identify on-line court users. In such circumstances users should be informed that their identity and activity is being tracked and this should take the form of terms of use that are accepted upon entry into the system.	Fairness, Human Dignity, Public Confidence

8.8 Security Policies

Security policies are designed to describe the terms surrounding the security of Court Information and to ensure that access is only possible in accordance with the access and privacy policies.

When considering security there is a general tendency to assume that threats come from malicious external intruders. However, the recent Wikileaks incident highlighted the perhaps more concerning and greater risk that can come from within an organization. While safeguards can be implemented through technology, it will generally be just as important to develop mitigation strategies that address the 'human' element behind such breaches through staff training and recruitment protocols, contractual arrangements and similar approaches.

[34] http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/juries&CISOPTR=31 The paper describes how multifaceted and nuanced the issue of juror privacy can be in contemporary society. A brief overview of relevant caselaw demonstrates a surprising lack of consensus about the importance that courts should ascribe to protecting the confidentiality of jurors' personal information. It then proposes a framework in which the principle criteria for determining whether juror information should be publicly accessible is whether that information is relevant to the juror's ability to be fair and impartial in the context of a specific trial. The framework is illustrated with a detailed description of whether information collected during various stages of the pretrial and trial process – summoning and qualification, voir dire, post-verdict — should be protected or disclosed.

Security Policies

Policy	*Rationale*	*Court Values Enhanced by Policy*
1. ***Judicial Information*** must be protected from unauthorised access in accordance with the CJC's Blueprint for the Security of Judicial Information.	• It is generally acknowledged that ***Judicial Information*** should be subjected to particularly rigorous security arrangements to ensure that it is inaccessible and remains strictly confidential. However, some ***judicial information*** can make a transition onto the Case File information or even Court Record. (For example, once a draft judgment is published it is effectively included on the Court Record however its previous draft version still remains within the realm of Judicial information. • The proposed definition for Judicial Information is contained in the glossary. The CJC's recent Blueprint provides some thorough guidelines as to how it might be protected. Note the inclusion of the new concepts within the definition to incorporate email, text messages, and voice-mail messages. It also includes web site usage history and social media content.	Independence, Public Confidence,
2. Oaths of confidentiality will be contained in engagement contracts for employees, consultants and contractors to prevent inappropriate disclosure of sensitive ***Court Information***.	• While such arrangements are unlikely to provide safeguards against purposeful leaks such as those behind the recent Wiki-leaks incident, they will at least alert those working in or with courts to the importance of keeping information confidential and to the inherent legal and personal risks involved in releasing information inappropriately.	Public Confidence, Independence
3. Audit logs will be closely monitored to clearly identify which users have access to ***Court Information*** at any point in time.	• Detect intrusion or unusual activity early and raise the alarm regarding possible security breaches • Closely monitor all requests for bulk data even if submitted from authorized sources • Preemptive monitoring of audit trails • Damage control once information is leaked..	Public Confidence, Independence
4. Staff Training Strategies should be embraced to improve awareness of the sensitivity of ***Judicial Information***		Public Confidence, Independence
5. ***Judicial Information*** should be subjected to additional protection over and above the security safeguards applied to ***Court Information***.	• The CJC's Security of Judicial Information Blueprint (currently under review) will provide a guiding framework. • This document is due for revision every two years • It will need to incorporate emerging issues such as the security of judicial email boxes, voice mail systems, text based communications and web browsing logs/history.	Integrity, Independence, Public Confidence

Security Policies

Policy	*Rationale*	*Court Values Enhanced by Policy*
6. Where a public wireless Internet access point is installed within a court precinct it must not compromise ***Court Information***.	• Many courts now offer wireless access points for the public within their courthouses • It is important to ensure that such 'public' Internet gateways are kept separate and distinct from court operational networks and communication infrastructure to minimize the risk that ***Court Information*** may be compromised. • Internet access should only be available to members of the public who are involved in court proceedings or who are otherwise granted access. • There should be some constraints around access to the Internet via such facilities (e.g. passwords and usernames issued by the registry) • The Judicial Information Technology Security Officer (JITSO) must sign off on such solutions prior to implementation and must also provide the judiciary with an acceptable risk assessment on a regular basis.	Public Confidence, Integrity

8.9 Preservation Policies

The different categories of Court Information identified earlier need to be preserved in accordance with their ongoing importance and the likelihood that they will need to be accessed over time.

The standards proposed by the Canadian Council of Archives and Library and Archives Canada should be used in terms of best practice guidelines.

The Canadian Council of Archives assumes leadership within the Canadian archival community and provides coordination and strategic planning. It advises the National Archives of Canada on national priorities, policies, and programs for the development and operation of a national archival system including such matters as:

- studies needed in developing the Canadian archival system;
- the establishment of principles, standards, and national priorities;
- the allocation of resources, grants, and services;
- the design of new programs, grants, and services to assist the development of the Canadian archival system;
- strategic planning to make the needs and concerns of the Canadian archival community better known to policy makers, researchers, and the public;
- and the coordination of joint projects within a national archival system.

The Preservation Policy released in 2001 by Library and Archives Canada states the principles that guide the preservation activities of the National Archives of Canada in fulfilling all aspects of its mandate. It gives direction to staff for carrying out their responsibilities regarding the preservation function and communicates the principles which guide preservation in National Archives.[35]

Preservation Policies

Policy	*Rationale*	*Court Values Enhanced by Policy*
1. Information held on the ***Court Record*** will be permanently preserved in accordance with best practice guidelines.	• International standards that have been mandated by the Canadian Council of Archives will be applied to ensure: - preserved information remains recoverable and accessible throughout the relevant retention period - the format in which the information is preserved is appropriate - the media used to preserve the information is appropriate - protocols and procedures surrounding the preservation process are well documented and represent best practice - responsibilities are well documented and communicated	Access, Public Confidence
2. Information held on the **Court File** that is not included on the ***Court Record*** will be retained for 20 years in accordance with best practice guidelines.		Access, Public Confidence
3. ***Judicial Information*** that is not included on the ***Court Record*** will be retained for 10 years and will be managed in accordance with best practice guidelines.		Access, Public Confidence
4. Privacy policies will be observed for ***Court Information*** that is preserved	• The obligation to protect Personal Identification Information from inappropriate access or disclosure applies equally to 'preserved' information and current or 'active' information.	Access, Human Dignity, Public Confidence

[35] http://www.collectionscanada.gc.ca/preservation/003003-3200-e.html

8.10 Performance Measurement Policies

Performance Measurement Policies

Policy	*Rationale*	*Court Values Enhanced by Policy*
Key court performance measures will include the following (by Case Type): • Clearance Rates • Time to Disposition • Age of Active Pending Cases • Age of Reserved Judgments	• The definitions and formula used to calculate these measures are contained in the glossary of terms. • Defining performance measurement criteria prior to system design will ensure that systems are built to capture the right information at the right time. This will maximize the potential to deliver accurate and efficient outcomes. • Building performance criteria into the design up front will also increase the likelihood that court systems will ultimately be able to deliver meaningful performance reports automatically without the need for time consuming, error prone, manual manipulation. • The unit to be counted for the purposes of performance measurement is a ***Court Case*** irrespective of the number of proceedings, actions, applications or motions contained within it. • A Case is not considered Finalized until all proceedings or matters contained within it are Finalized. • Clearance Rate = New Filings plus Re-opened Cases minus (Cases Finalized by Judgment plus Cases Finalized by other means e.g. Settlement, Withdrawal, Abandonment, Discontinued) • Time to Disposition = Median Time from Initiation of Case to Finalization of Case • Age of Active Pending Cases is shown as a median value • Age of Reserved Judgments is shown as a median value	Transparency, Efficiency, Effectiveness, Public Confidence

APPENDIX 1: REFERENCES

The Canadian Judicial Council's Third Edition of the Blueprint for the Security of Judicial Information[36] prepared by the Computer Security Subcommittee of the Judges Technology Advisory Committee and released in 2009.

The Canadian Judicial Council's Model Policy for Access to Court Records in Canada (2005)

The The CJC's Model Access Policy (above) was based on a 2003 CJC discussion paper called: "Open Courts, Electronic Access to Court Records, and Privacy".

Austin, Lisa M. and Pelletier F., Synthesis of the Comments on Judges Technology Advisory Committee's Discussion Paper on Open Courts, Electronic Access to Court Records and Privacy, Canadian Judicial Council, January 2005.

Court Information Act 2010, No 24 New South Wales, Australia

New Zealand Law Commission (NZLC) Access to Court Records Report No. 93 (2006) leading to establishment of new court rules for New Zealand courts in 2009.

Judith Bellis – Public Access to Court Records in Australia: An international comparative perspective and some proposals for reform. 19 (4) (April 2010) Journal of Judicial Administration 197-231

Reviewing PIPEDA: Control, Privacy and the Limits of Fair Information Practices, Lisa M. Austin, Faculty of Law, University of Toronto. Paper originally presented at the 35th

Annual Workshop on Commercial and Consumer Law University of Toronto, October 22, 2005

Alberta Courts – Public and Media Access Guide – November 2009

US Department of Justice – Justice Reference Architecture – Version 1.7 – March 2009 – Global Infrastructure/Standards Working Group

The Alberta Courts Services Retention and Disposition Schedule, 2006/002

The Imperative of Incorporating Privacy Protections at the Design Stage Special Guest Columnist Daniel Caron, Legal Council for the Office of the Privacy Commissioner of Canada JURIST Side Bar - http://jurist.org/sidebar/2010/01/new-innovative-technologies-that-raise.php

Privacy, Trust and Innovation – Building Canada's Digital Advantage - Submission from the Office of the Privacy Commissioner of Canada to the Digital Economy Consultation July 9, 2010 http://www.priv.gc.ca/information/pub/sub_de_201007_e.pdf

Personal Information and Electronic Documents Act (PIPEDA) SC 2000 c 5.

The Privacy Payoff: How Successful Businesses Build Customer Trust, Ann Cavoukian Ph.D. and Tyler Hamilton, McGraw-Hill (2005)

[36] http://www.cjc-ccm.gc.ca/cmslib/general/JTAC-ssc-Blueprint-Third-edition-finalE.pdf

Privacy Designs Principles for an Integrated Justice System – Working Paper (April 2000), Ann Cavoukian Ph.D. www.ipc.on.ca/index.asp?layid=86&fid1=326

Privacy Impact Assessment for Justice Information Systems (August 2000): www.ipc.on.ca/index.asp?layid=86&fid1=318

Privacy by Design – Take the Challenge, Ann Cavoukian Ph.D. Information and Privacy Commissioner of Ontario, Canada http://www.privacybydesign.ca/content/uploads/2010/03/PrivacybyDesignBook.pdf

Global Justice Information Sharing Initiative: Exploring Service-Oriented Architecture Services for Justice Information Sharing http://it.ojp.gov/documents/soa_services.pdf

US Department of Justice's Global Justice Information Sharing Initiative, 15 December 2008

The CJC's Use of Personal Information in Judgments and Recommended Protocol http://www.cjc-ccm.gc.ca/cmslib/general/news_pub_techissues_UseProtocol_2005_en.pdf , March 2005

The Supreme Court of the United Kingdom policy statement regarding "The Use of Live Text-Based Communications from Court" http://www.supremecourt.gov.uk/docs/live-text-based-comms.pdf

Canadian Bar Association - Information to Supplement the CODE OF PROFESSIONAL CONDUCT Guidelines for Practising Ethically with New Information Technologies, September 2008 http://www.cba.org/CBA/activities/pdf/guidelines-eng.pdf#page=13

Making the Case for Juror Privacy: A New Framework for Court Policies and Procedures* by Paula L. Hannaford http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/juries&CISOPTR=31

Horrific Video Tapes as Evidence: Balancing Open Court and Victim's Privacy – Bruce A. MacFarlane, Q.C. Deputy Minister of Justice Deputy Attorney General for the Province of Manitoba September 25th, 1998 [Originally published in 41 Criminal Law Quarterly 413 (1999)] http://www.canadiancriminallaw.com/articles/articles%20pdf/Horrific_Video_Tapes_as_Evidence.pdf

APPENDIX 2A: ALLOCATION TABLE FOR THE COURT RECORD AND CASE FILE

This table provides an example of an approach to classification that could be embraced within any jurisdiction to determine the information and documents to be included on the ***Court Record*** as compared with the ***Case File***.[37]

It also provides a mechanism to challenge the established practice of including potentially large volumes of material on the ***Case File*** that may be irrelevant for the court's purposes (e.g. subpoenaed material). Rather than ask, how should we manage such information, the question might properly be constructed as "Why do we receive this information in the first place and does the court really need it?"

The values entered in the table involve important policy decisions for the policy makers within each jurisdiction and are likely to generate some debate. It will be necessary for the policy makers within each jurisdiction to complete the table in accordance with the local landscape, prevailing policies, legislative and other constraints.

It is important to note that the **data entered in the table below is provided by way of example only and is not meant to be prescriptive.** It will be a matter for the policy makers in each jurisdiction to complete such a table and different courts may come to different conclusions. For example; policy makers in some jurisdictions may consider drafts of orders or communication back and forth between the judge and counsel should be broadly accessible to the public while others may consider it only appropriate for the parties.

It is also important to note that privacy policies will take precedence over the various allocations made in the table below. For example; where a self-represented person files a notice of appeal, this will become part of the ***Court Record*** as the initiating document. However, the person's address for service will not become part of the ***Court Record***. It will be available on the ***Case File*** so that those who need it, for example, to make service, will have access to it, however it will not be available to the general public upon enquiry.

[37] See definitions in Appendix 3.

Information or Document Description	*Is this really needed by the court? (in light of the minimal collection principle)*	*Part of the Case File? (Accessible to the parties – limited preservation – restricted access information)*	*Part of Public Court Record? (accessible to the public, preserved indefinitely – open access information)*
Pleadings *(e.g. Statement of Claim, Statement of Defence etc)*	Yes	Yes/No	Yes
Initiating Documents	Yes	Yes/No	Yes
Issued Orders, Rulings and Judgments & published reasons for Judgment	Yes	Yes	Yes
Submissions	Yes	Yes	Yes/No?
Draft Orders prepared by parties for consideration of judge	Yes	Yes	Yes/No?
Draft Orders prepared by judge for consideration of parties	Yes	Yes	Yes/No?
Paper Correspondence (fax or post)	Yes	Yes	Yes/No?
Email Correspondence	Yes	Yes	Yes/No?
Judicial working notes / Aide memoirs	Yes	Yes	No
Affidavit of Documents, Discovery List	No?	Yes	No
Lists of Authorities	Yes	Yes	No
Copies of Authorities	Possibly	Yes	No
Affidavits tendered with or without exhibits *(but not admitted in evidence)*	Possibly	Yes	No
Reasons for Judgment	Yes	Yes/No	Yes
Draft Judgments	Yes	No	No
Transcript	Yes	Yes	Yes
Criminal record of the Accused	Yes	Yes	No
Expert Reports	Possibly	Yes	No unless relied upon by Judge
Indictments or Charge Sheets	Yes	Yes	Yes
Pre-Sentence Reports	Possibly	Yes	Yes/No?
Medical and psychological reports	Possibly	Yes	No
Child Custody Investigations	Possibly	Yes	No
Subpoenaed material	No	No unless expressly required by court	No unless relied upon by Judge
Docket Information *(e.g. Court Events, judicial officer, orders, appearances)*	Yes	Yes/No	Yes/No
Prescribed forms (per Court Rules)	Possibly	Yes/No	Yes/No

Information or Document Description	***Is this really needed by the court?*** *(in light of the minimal collection principle)*	***Part of the Case File?*** *(Accessible to the parties – limited preservation – restricted access information)*	***Part of Public Court Record?*** *(accessible to the public, preserved indefinitely – open access information)*
Extracts of Key Evidence *(as used in Appellate jurisdictions)*	Yes	Yes/No	Yes/No
Bills of Costs	No	No	No
Legal representation status	Yes/No	Yes/No	Yes/No
Result (i.e. Proceeding outcomes)	Yes/No	Yes/No	Yes/No
Listing History - Events, Outcomes & Appearances	Yes	Yes	Yes
Contact details for legal representative (firm)	Yes	Yes	Yes
Contact details for legal representative (person)	Yes	Yes	No
Contact details for represented litigants	No	Yes/No	Yes/No
Contact details for unrepresented litigants	Yes	Yes	No
Contact details for witnesses, jurors, victims	Yes/No?	Yes	No
Accused name and address	Yes	Yes	Yes/No
Convicted person's name	Yes	Yes	Yes/Yes
DOB & Address for persons accused	Yes	Yes	Yes/No
DOB & Address for persons convicted	Yes	Yes	Yes/No
Accused Unique Person Identifier *(this is simply an internal linkage data field for use across justice systems)*	Yes	Yes	No

APPENDIX 2B: USAGE OF COURT INFORMATION MATRIX

Case Type (e.g. Juvenile)	*Judicial Information*	*Case File*	*Court Record*	*Court Docket*
		Restricted Access Information	*Open Access Information*	
Judiciary	CRUD	CRUD	CRUD	CRUD
Registry		CRUD	CRUD	CRUD
Parties		RU	RU	RU
Media			R	R
Public			R	R
Criminal Justice Agencies		RU	RU	R
Witnesses			R	R
Jurors			R	R
Unauthorised Publishers / Distributors / Aggregators / Search Engines			RD	RD
Authorised Publishers / Distributors / Aggregators			RDP	RDP

Access Categories include **C**reate **R**ead **U**pdate **D**istribute (as-is) Re**P**ackage (e.g. rebundle, extract metadata / add value to achieve commercial outcome)

The ***Court Participants and Users*** identified in the above table are defined within the definitions section of this document. The values completed in the Usage of Court Information Matrix above are for demonstration purposes only as this will involve important decisions for the policy makers within each jurisdiction.

A Usage of Court Information Matrix should be completed for each of the major ***Case Types*** that are commonly managed within a jurisdiction.

APPENDIX 3: RECOMMENDED KEY DEFINITIONS

The key terms that are required to support the information management policy framework are identified below along with proposed definitions.

It is acknowledged that further elaboration, interpretation and practical precision will be necessary from jurisdiction to jurisdiction. This is likely to necessitate some modification and sub-definition work to ensure the defined terms can be used in a practical context within each jurisdiction. It is not viable to micro-predict or direct detailed definitions at a national level.

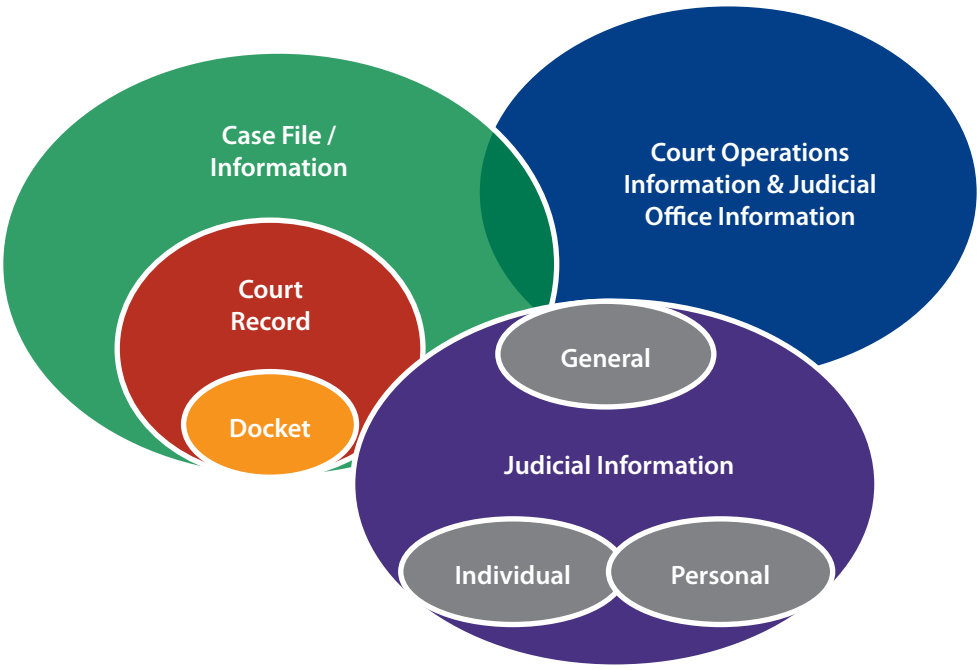
The definitions presented below have been endorsed by the Canadian Judicial Council's Administration of Justice Committee. A Definitions Working Group was established by the Committee to finalize the definitions in August 2011. The Working Group took into account recommendations of the CJC's Administrative Efficiency in Trial and Appeal Courts Sub-committee.

The definititions are designed to be *medium neutral* in so far as they should apply equally to information held in paper format and to information held in digitized format in case management databases, intranets, document management systems, on computer network servers, electronic storage devices and in email repositories or electronic diaries and calendars.

Court Information

The diagram below identifies some of the main terms regularly used in relation to court information and provides a graphical representation of the inter-relationships between these common terms.

Diagram 4 : Court Information Terms and Inter-relationships



Case Information

Case Information includes all information associated with a ***Case File*** whether permanent, as being part of the ***Court Record***, or transitory, as having been associated with the ***Case File*** but not being part of the ***Court Record***.

Case File Management includes the management of the ***Case File***, the ***Court Record*** and the ***Court Docket***.

Judicial Case Management includes ***Case File Management*** and management of ***Judicial Information***.

Court Operations Information

Court Operations Information is information relating to general court administration including:

a) listing of court proceedings in relation to one or more case;

b) court calendars;

c) work produced by registry executives, managers and staff;

d) court staff HR matters;

e) facilities management;

f) IT infrastructure management;

g) statistics; and

h) security.

Court Operations Information is not part of the Court Record unless a Judicial Officer expressly so directs and only to that extent.

Judicial Office Information

Judicial Office Administration includes judicial staff HR matters, judicial assignment information, statistics and court policies.

Judicial Office Information is not part of the Court Record unless a Judicial Officer expressly so directs and only to that extent.

Case

A ***Case*** refers to a single legal proceeding initiated in court and assigned a unique file number for that court. A ***Case*** may be related to other ***Cases*** by overlapping matters or parties. A ***Case*** may involve multiple matters and multiple steps in the proceeding.

Case File

The Court may maintain a ***Case File*** for each Case, whether electronic or paper, or a combination of both, which shall contain the ***Court Record*** and may include the following transitory ***Case Information***:

a) personal information;

b) correspondence;

c) financial transaction information;

d) an index of file content;

e) minutes and log notes by court staff; and

f) any applicable information contained in the electronic case management system.

Court Record

The Court has a duty to maintain a ***Court Record*** of each Case, whether electronic, paper, or a combination of both, where:

a) a) it is a permanent element of the proceeding before the court;

b) b) it is retained under statutory authority or administrative principles of the court; or,

c) c) it has a legal significance for the future.

The ***Court Record*** shall include the ***Court Docket*** and may include:

a) all documents related to the ***Case***, including correspondence, submitted for filing in any form;

b) information that relates to particular ***Cases*** or proceedings such as motions, orders, judgments and reasons for judgment, endorsements, affidavits;

c) exhibits lodged on ***Case Files*** whether or not they have been accepted in evidence subject to statutory authority or a Court's retention policy;

d) any written jury instructions given or refused;

e) court reporters' notes, audio or video recordings of court proceedings, and any transcripts prepared from them;

f) an index of file content;

g) minutes and log notes by court staff; and

h) any applicable information contained in the electronic case management system.

Court Docket

A ***Court Docket*** is a sub-set of the ***Court Record*** and provides the chronology of events relating to a particular ***Case***. It includes:

a) a description of each event;

b) name of the presiding Judicial Officer

c) dates and times of the event

d) names of parties or legal representatives in attendance;

e) orders made, judgments delivered; and

f) documents tendered and accepted into evidence.

Judicial Officer

A ***Judicial Officer*** is a person acting in a judicial or quasi-judicial capacity including judges, deputy judges, masters, justices of the peace, registrars, prothonotaries or anyone else authorised to act in an adjudicative role.

Judicial Information

Judicial Information is information stored, received, produced or used by or for a Judicial Officer. It also includes information stored, received, produced or used by staff or contractors working directly for or on behalf of judges such as executive officers, law clerks, law students, judicial clerks or assistants. There are three main types of Judicial Information:

> ***Individual Judicial Information*** includes work product, research material and professional development information of of staff Lawyers, Law Clerks and Judicial Officers.
>
> ***General Judicial Information*** includes information used by Chief Justices, committee materials, statistics, research material, and court-wide professional development information.
>
> ***Personal Judicial Information*** includes information produced by, on behalf of, or relating to a Judicial Officer that does not directly relate to the function or role of the Judicial Officer and is not associated with a Case.[38]

Any judicial information that falls outside these three categories that is lodged on a Case File (for example; orders or published reasons for judgment) becomes ***Case Information*** once it is inserted into the ***Case File***.

Personal Information

Personal information means information that may be used to establish a person's identity or to obtain access to information relating their private and personal affairs including:

a) financial account numbers and records;

b) tax file numbers and returns;

c) social insurance numbers;

d) finger print numbers;

e) driver's licence numbers;

f) medical insurance numbers;

g) financial account numbers;

h) passport numbers;

i) personal telephone numbers;

j) date of birth;

k) home address;

l) personal email addresses; and

m) any other information that can be used to establish a person's identity.

---

[38] The Administration of Justice Committee's Definitions Working Group concluded that it was not useful to venture a detailed definition of Personal Judicial Information beyond this. In each jurisdiction, it will be necessary to provide precise guidance to technologists in relation to Judicial Internet browsing history logs, email repositories, contact lists, calendars, text messages and voice mail when considering candidate information for this category.

Case Status

A Case can either be active, closed or archived. Status will be a key feature in statistical analysis, audit and performance measurement by each court. Each jurisdiction will determine the status of a Case according to its local criteria and any applicable law.

Each Matter or step in a Case may also be active or closed. Each jurisdiction will also determine the extent to which such status will be relevant to statistical analysis, audit or performance measurement.