Update on "Judicial Writing in an Electronic Age" – Five Years On*

[1] My original paper "Judicial Writing in an Electronic Age"[1] was written in December 2004 at an early stage of the identification of some negative consequences of electronic publication of judgments and sentencing remarks[2] and the development of strategies to address those consequences. This paper updates some of the developments that have occurred in the meantime and suggests further issues for consideration.

What is the problem?

[2] Judgments frequently contain personal information about the parties or witnesses which has usually been included in the judgment as essential background or part of the explanation to explain the decision. Prior to electronic publishing, most judgments were not published and were obtainable only from the parties, their lawyers, court files or court library collections. Electronic publication has facilitated wide dissemination of and accessibility to judgments. This promotes the concept of open justice and the transparency and accountability of the justice system, but also preserves and makes available in the public domain the personal information about the parties and witnesses.[3] The two main negative consequences of electronic publication for judgment writing are:

(a) infringement of the privacy, or embarrassment, of litigants and witnesses; and
(b) the potential for contributing to identity crime.

---

* This paper was presented at the South Australian Judicial Development Day at Adelaide on 3 December 2009.

[1] Justice Debra Mullins "Judicial Writing in an Electronic Age" (Speech delivered at the 2005 Supreme and Federal Courts Judges' Conference, Darwin, 26 January 2005)

[2] I will use the expression "judgments" to cover both judgments and sentencing remarks, where appropriate.

[3] Spigelman JJ, "Open Justice and the Internet" (Speech delivered at the Law Via the Internet 2003 Conference, Sydney, 28 November 2003)

Court policies and protocols

[3] Some courts and judicial bodies have developed policies or protocols on the electronic publication of judgments that are directed at minimising the negative effects of accessible personal information. In some instances, these policies or protocols are internal documents available for reference by judges and their staff, but not publicly available.[4]

[4] In March 2005 the Canadian Judicial Council (CJC) approved the "Use of Personal Information in Judgments and Recommended Protocol".[5] The CJC Protocol addresses three levels of protection that are set out in paragraph [21]:

> A. **Personal Data Identifiers:** omitting personal data identifiers which by their very nature are fundamental to an individual's right to privacy;
> B. **Legal Prohibitions on Publication:** omitting information which, if published, could disclose the identity of certain participants in the judicial proceeding in violation of a statutory or common law restriction on publication; and
> C. **Discretionary Protection of Privacy Rights:** omitting other personal information to prevent the identification of parties where the circumstances are such that the dissemination of this information over the internet could harm innocent persons or subvert the course of justice.

[5] For the purpose of this paper, I propose focusing on matters covered by paragraphs A and C of the CJC Protocol. Most courts have developed systems for ensuring that judgments that are made available for electronic publication comply with suppression orders and statutory or other restrictions on publication of the identity of participants.

---

[4] I have had the advantage of being able to consider the section on Anonymisation of Judgments in the New Zealand Court of Appeal Judges' Manual (current as at 14 September 2009)

[5] "Use of Personal Information in Judgments and Recommended Protocol" (approved by the Canadian Judicial Council March 2005).

[6] One of the objectives of the CJC Protocol was to address the protection of personal information of judgments and thereby encourage courts to publish all their decisions on the internet. The preference was also expressed for Judges to address these issues when their decisions were drafted.[6]

[7] A number of Canadian courts have adopted the CJC protocol or similar guidelines.[7]

[8] The New South Wales Supreme Court published its "Identification Theft Prevention and Anonymisation Policy" on 10 December 2007.[8] This policy extends to transcripts in addition to judgments. The purpose of the policy is to prevent identity theft in relation to litigants and witnesses involved in court proceedings and to anonymise the identities of accused persons and witnesses in appropriate cases. Paragraph 3.2 of the policy suggests that judges should consider anonymising the types of information that are set out in that paragraph, as a matter of practice:

> 1. Residential addresses of all victims, witnesses and parties should be omitted if it has no relevance to the case. Addresses of the accused should be omitted or anonymised if this will lead to the identification of the victim.
> 2. Dates and places of birth of victims and witnesses should be anonymised or omitted.
> 3. Residential history of accused and victims should be anonymised if this could lead to identities being revealed, eg, 'the family moved from Queensland to NSW. They lived in Wagga and then moved to a dairy farm in Berry. They then bought a property in Nowra and lived in the garage for 9 months while the house was being renovated.'
> 4. Anonymise one or both sets of information if a victim or accused is easily identified because they come from a minority group in a small town. Eg. The accused is

---

[6] CJC Protocol, paragraph [18].
[7] Court of Queen's Bench of Alberta "Notice to the Profession, Resumption of Publication of Family Law Judgments of the Court of Queen's Bench on the Alberta Courts Website" (26 July, 2006); British Columbia Court of Appeal "15. Guidelines for Protecting Privacy Interests in Judgments" (29 June 2004)
[8] Supreme Court of New South Wales "Identification Theft Prevention and Anonymisation Policy" (published 10 December 2007)

of Tongan descent and has been living in Numbugga for 3 years.

5. Omit or anonymise names of schools and places of work if it has no relevance to the case.

[9] Although paragraph 3.2 sets out desirable practices for a judge in judgment writing, section 4 of the policy mandates that a judge's staff and the Reporting Services Branch must, unless otherwise directed by a Judge, use the substitution techniques for unique identifiers that are set out in that section. It covers dates of birth and anniversaries, all types of addresses (property numbers, telephone numbers, email addresses, fax numbers) and unique numbers such as for a bank account, tax file number, Medicare, credit card or passport.[9]

[10] The New Zealand Court of Appeal in *White v Northumberland* [2006] NZFLR 1105 endorsed the approach of giving made up names to the parties for the purpose of the future citation of the case, rather than using letters. This was explained at paragraphs [63] and [64]:

> [63] In *Brown v Argyll* [2006] NZFLR 705, Priestley J referred to the difficulty for family lawyers in coping with case names which are frequently a jumble of initials. The need for initials stems from the reporting restrictions imposed, for good reason, by s 139 of the Care of Children Act. Priestley J's solution was to make up names under which the case could be reported. In that case, both Brown and Argyll were such made-up names. We endorse that idea. It seems a better solution than that which the English have adopted to cope with this problem: examples of their solution can be seen above at, among other places, [23], [25], and [30].
>
> [64] In this case, we have given the child who is the subject of this proceeding a made-up first name. We have also suggested that the case could be cited as *White v Northumberland.* Those are not, of course, the parties' real names.

[11] The Family Court of Australia and the Federal Magistrates Court of Australia have addressed the statutory restrictions that apply to publication of proceedings under

the *Family Law Act* 1975 by using pseudonyms in place of party names for publication purposes and developing anonymisation guidelines.[10] The choice of pseudonym can itself be problematic.[11]

Identity crime

[12] An electronic database of judgments is one of many databases available to those who are willing to commit an identity crime. The nature and impact of identity crime is discussed in the Final Report on "Identity Crime" prepared by the Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General (SCAG).[12] The term "identity crime" is now used as a generic term covering identity fraud and identity theft and describes activities in which a perpetrator uses a fabricated identity, a manipulated identity, or a stolen/assumed identity to facilitate the commission of a crime.[13] Appreciation of this potential for fraudulent manipulation of publicly available personal information justifies the exercise of caution by judges and courts in disclosing unnecessary personal information in court databases.

---

[9] Recent examples of the application of the New South Wales policy are *S v State of New South Wales* [2009] NSWCA 164 and *Perpetual Ltd v Karen Treloar* [2009] NSWSC 386

[10] Lyn Newlands, "Lifting the veil – the changing face of judgments publishing in the Family Court of Australia" (Paper delivered at the 2009 Australian Law Librarians' Association Evolution Conference, Darwin, 2 to 4 September 2009)

[11] For example, see: *Dmitrieff & Shaw and Ors* [2008] FamCA 881 at [19] and [20]

[12] Standing Committee of Attorneys-General, Model Criminal Law Officers' Committee "Final Report Identity Crime" (March 2008) which was referred to by Spigelman CJ in *Stevens v R* [2009] NSWCCA 260.

[13] Standing Committee of Attorneys-General, Model Criminal Law Officers' Committee "Final Report Identity Crime" (March 2008) at p 8.

Spent convictions

[13] SCAG finalised its spent convictions project with the public release of the Model Spent Convictions Bill on the SCAG website on 6 November 2009.[14] The *Spent Convictions Bill* based on the Model Bill was introduced in the South Australian House of Assembly on 24 September 2009, passed in the House of Assembly and has been received in the Legislative Council. The Bill addresses the problem created by websites such as CrimeNet[15] by making it an offence for such a business to disclose information about a spent conviction in certain circumstances. Section 13 of the Bill provides:

> **13 Unlawful disclosures—business activities**
> (1) A person is guilty of an offence if—
> (a) the person, in the course of carrying on a business that includes or involves the provision of information about convictions for offences, discloses information about a spent conviction; and
> (b) the person knew, or ought reasonably have known, at the time of the disclosure, that the information was about a spent conviction.
> Maximum penalty: $10 000.
> (2) It is a defence to a charge for an offence against subsection (1) to prove—
> (a) that the disclosure forms part of the ongoing disclosure of the information in materials or in a manner that cannot be reasonably altered to remove information about the spent conviction; and
> (b) that the disclosure of the information commenced before the conviction became a spent conviction.

Restrictions on searching

[14] The use of the Robots Exclusion Protocol has been maintained by AustLII.[16] Enquiries made of the various courts for the purpose of this paper have ascertained that the Australian Capital Territory does not presently use the Robots Exclusion

[14] Standing Committee of Attorneys-General "Spent Convictions Model Bill" (September 2009)
[15] www.CrimeNet.com.au (accessed 1/12/09)
[16] Australasian Legal Information Institute "Privacy Policy" (Last updated: 31 July 2003; accessed 30/11/09)

Protocol for judgments on its website, but will use the protocol for excluding judgments, when its new website is launched in February 2010.

Privacy considerations

[15] When considering the extent to which the electronic publication of judgments should transcend the privacy considerations of those involved, account can be taken of the differences between parties and other witnesses.

[16] Parties to litigation (whether as plaintiff or defendant) are participating in a public process and, as such, must usually expect their participation to be a matter of record and open to public examination. This permits accountability of the process and the administration of the justice system. The prospect of this public scrutiny, whether in respect of the fact of the proceeding, the progress of the proceeding, evidence given at the trial, the outcome, or the reasons for the outcome, is a factor in containing the number of cases that commence, or proceed to a trial, or proceed to judgment. This is because a party who wishes to avoid the publicity that can be associated with a court proceeding, trial or judgment will be inclined to settle a civil dispute.

[17] As witnesses who are incidental participants in the litigation will usually not be participants by choice, the inconvenience or potential embarrassment of their participation can be minimised by keeping the information about them and their evidence to that which is essential to reaching the decision. Rarely will the full name of a witness be essential to the decision. Using the surname of the witness will be sufficient in most cases. In some matters, it may be sufficient to refer to the

witness by the role that the witness played in the events, eg the bus driver, the neighbour, the plaintiff's sister.

[18] Victims of crime and relatives of defendants in criminal matters may appropriately be described in many cases as innocent bystanders. Their details may be referred to in court. It is not uncommon practice for a judge to refer to the names of family members when sentencing a defendant or refer to the complainant's name and address in the sentence or a related proceeding. What is the public interest in keeping those details in the version of the sentence or a related proceeding that is published electronically?

[19] Where the balance lies between the public interest in open justice and the privacy considerations affecting parties, witnesses and their families will vary with the type of case. There are some categories of case, such as family provision applications or applications for statutory wills, where the issues revolve around personal relationships and full details of financial and personal circumstances. In those cases, personal information must be disclosed in order to expose properly the reasoning. Even so, the personal facts can be limited to those that were relied on in deciding the case, rather than reciting every one of the personal facts that was disclosed in the course of the evidence.

How does endeavouring to minimise personal information in judgments affect judgment writing?

[20] Judgment writing is not an easy task. On one view, balancing public interest and privacy considerations whilst writing the judgment makes the task more complicated. Another view is that it focuses attention on the aspects of the evidence

that are essential to the reasons and can streamline the reasoning by reducing unnecessary details.

[21] A threshold issue is whether the case is one in which it is appropriate to minimise references to personal information.

[22] Eliminating unique identifiers (such as full street address or full email address) is relatively straightforward. Consideration can also be given to whether it is sufficient to use identifying details that are general, rather than specific, in nature, such as "The plaintiff lives in a town in central Queensland" rather than "The plaintiff lives in Emerald".

[23] Care is required when incorporating quotes into judgments, such as extracts from medical reports or from the transcript of the evidence, to avoid inadvertent disclosure of personal information that is within the quote.

[24] Relating aspects of a witness' history in a judgment may reflect adversely on others who can be connected with the witness by readers of the judgment who may be acquainted or know of the witness. Consideration should be given to expressing that part of the witness' history in a way that minimises speculation. One example is where a plaintiff's history includes an allegation that the plaintiff was sexually abused by a family member and the history of childhood sexual abuse is relevant to the current proceeding. Recording that the plaintiff claims that he or she was sexually abused by a family member may lead a reader of the judgment to speculate on which family member was the alleged perpetrator. In a case where the identity of the perpetrator is not relevant, the history could be limited to reciting that the plaintiff claims to have been sexually abused as a child.

[25] It is important that minimising references to personal information is done in a way which leaves the judgment readable and reveals the true reasoning.

Issues

[26] As a result of looking at some of the protocols and guidelines used by courts for electronic publication of judgments and the content of court webpages, I suggest consideration of the following issues:

(a) should a judge be primarily responsible for reviewing his or her judgment for privacy considerations before it is published electronically?
(b) should a court have any other process for checking the content of a judgment to ensure that unique identifiers and unnecessary personal information are not included in the judgment that is published electronically?
(c) where a court does not make all its judgments available electronically, should the court disclose the criteria that are applied to determine what judgments are available electronically?
(d) if the court anonymises judgments, other than those that are covered by statutory prohibitions on publication, should the court publish the criteria that are applied for determining that a judgment is appropriate for anonymisation?

Justice Debra Mullins
Supreme Court of Queensland
2 December 2009