SECURITY AND PRIVACY ISSUES RELATING TO TECHNOLOGY AND THE LAW

1. INTRODUCTION

The use of computer technology in legal procedures necessarily gives rise to issues relating to the security and privacy of electronically transmitted and stored information. Often in the course of a legal matter, information of a personal nature is disclosed such as business, family or medical details. A natural concern of parties revealing such information will be to ensure that it is only used for a specific purpose and not unnecessarily disclosed or accessed. The potential for the unauthorised use of sensitive information is of increased concern where it is stored and transmitted electronically. This is due in part to the greater amount of information able to be stored, and in part by new security risks to material when in electronic form. Issues of privacy also arise in the context of electronic publication of law reports. The greater accessibility of law reports which this technology can offer, also mean that any personal information contained within the report is able to be more readily obtained.

As well, it is important that there is some method by which the author of an electronic document can be reliably ascertained. In particular, for a communication to be relied upon it must be possible to demonstrate with a high degree of certainty that a document has not been tampered with or altered in some way.

It is important that such concerns are addressed in order to guarantee the integrity of any electronic legal system and to establish confidence in the reliability of the system. Without sufficient guarantees of security and a respect for the privacy of information, the development of electronic legal procedures is unlikely to be readily accepted by the legal profession and the wider community.

Part 2 of this report addresses issues of privacy in terms of ensuring the security of electronically transmitted and stored data. In doing so, it outlines the level of protection required by the current legal framework. It then considers how the required legal standard could be satisfied with current available technology. finally, an assessment is made as to whether this level of protection is sufficient to allay any security concerns arising in electronic legal processes.

Part 3 of this report considers privacy concerns in relation to the disclosure of personal information via electronic law reports. It sets out the reasons underlying the publication of law reports and the current law which permits the suppression of information in law reports. Finally it considers whether the current law offers an appropriate means by which to address concerns of privacy which may arise.

2. PRIVACY — Ensuring the Security of Stored and Transmitted Data.

1. *Interception.*

In a system of e-filing, documents may be exchanged between numerous parties and computer systems. These include transmissions between client, legal practitioners and the Court and transmissions between individuals within a legal practice or client company. Modes of document transmission may vary from the exchange of floppy disks or CDRoms, transfer via a LAN or intranet system or transfer via the Internet or an extranet system.

The possibility of interception of electronic communications in the context of an e-filing system potentially limit its capacity to serve those involved in legal proceedings. This is obvious in the context of potential disclosure of confidential client/ legal practitioner communications and the effect of such a disclosure on any ensuing proceedings. Risk of interception also reduces confidence that any communication with the court has in fact been received. Without sufficient safeguards court processes may be interfered with.

Where communication is by the exchange of floppy disks or CDRoms, the risk of interception may be no greater than is currently the case with traditional forms of communication. Where information is exchanged over a network, the communication is conducted over shared communication lines. This means that it is possible for an outsider to program their computer system to receive copies of messages exchanged between two parties. It is also possible for an outsider to configure their computer to emulate that of the intended recipient of a message. This allows the third party act to as an impostor and to intercept messages intended for the recipient. They can also reply to the sender in the name of the intended recipient, giving the impression that the message was properly received.

Even if the content of the message is not able to be viewed by the outsider, they may still be able to determine attributes of the communication such as the time, amount of information exchanged and the parties involved.

2. *Storage of Information.*

Currently, personal information relating to legal proceedings is kept stored by the Courts and legal practitioners long after the matter has been closed. Electronic storage increases the ease and reduces the expense of storing larger amounts of information. A change from paper to electronic records requires a change in the security procedures and devices protecting stored information. As well, it is important to ensure

that better storage mechanisms do not result in information being stored for longer than is actually required. The longer information is stored the greater the risk that it will be used for unauthorised purposes.

3. *The Legal Framework.*

There are two main ways in which the law operates to ensure that information is only used for authorised purposes. The first is by imposing criminal or civil sanctions upon those gaining access to sensitive information with permission. The second is by required the party holding the information to ensure that it is handled in accordance with certain standard of security and privacy.

1. Criminal and Civil Sanctions.

To some extent the integrity of electronically communicated information can be ensured by deeming any interceptory conduct to be an offence. Such measures have been included in the Electronic Commerce Framework Bill 1997 (Vic) which would amend the Crimes Act 1958 (Vic) to include offences such as the gaining of access to data without authorisation, or with an intent to defraud, or where the offender knew or ought to have known that the data was of a sensitive nature. This Bill is due to be introduced into Parliament in the Autumn Session 1999. These provisions will add to the existing legislative regulation of computer crimes at both federal and state level. General law actions in trespass, breach of confidentiality, conversion and negligence may also be available against those who gain unauthorised access or cause damage to data and provide remedies in the form of compensation for loss or injunctions against further disclosure of information.

While this legal framework is no doubt of assistance, its effectiveness in protecting the security of electronic information is limited. In practice, the nature of computer crimes gives rise to particular problems their enforcement. Investigators face new challenges in establishing the identity of offenders, in the collection of sufficient evidence to result in prosecution and in acting against offenders who are outside the legal jurisdiction.

Detailed inquiry into methods for improving the effectiveness of prosecuting computer crimes is beyond the scope of this report. Work in this area is no doubt important in increasing the security of electronic technology as any increase in the likelihood of punishment for a breach of the law is likely to have a deterrent effect upon potential offenders. Yet it is considered that sanctions are largely reactive in nature and as such are of themselves, inadequate to fully address concerns

regarding the prevention of a breach in the security and privacy of electronic information. As such, this report will focus upon the way in which the law is able to ensure more pro-active security and privacy measures are adopted so as to prevent any unauthorised access of data.

2. Current Required Standards of Security and Privacy.

1. *Duty of Confidentiality.*

There is no general right of individual privacy recognised at common law. However, some protection of information is offered in particular areas by various privileges and duties. At both general law and under the Legal Practice Act 1996 (Vic) s 64(c), a legal practitioner has a duty to maintain the confidences of their clients. In particular, confidential information imparted in circumstances giving rise to an obligation of confidence may be legally protected.

This protection currently extends to most client information held by legal practitioners. While generally, information given to the court may be of a public nature, clearly in certain cases the information will not be intended to be publicly disclosed. More obvious examples include, applications to the court by investigating officials to wire tap suspects, matters involving trade secrets and information given by complainants in sexual offence cases. Should this confidential information be electronically stored or transmitted by the court, then a duty would most likely be owed to ensure that reasonable precautions are taken to ensure no persons have unauthorised access.

Where there is or is likely to be an unauthorised use of the confidential information the court may prevent disclosure using injunctive relief, the delivery up and destruction of the information or the compensation for any loss of the plaintiff arising as a result of the breach.

It remains open to question whether interception of information communicated via e-mail would be deemed of a sufficiently confidential nature so as to be protected by a duty of confidence. An analogy may be drawn with English and US decisions where it has been held that parties communicating over the telephone accept the risk of their communication being intercepted. However this approach has been criticised. The New Zealand Law Reform Commission, has concluded that such communications are of a confidential nature. Given the uncertainty of the law in this area and the growing ease

by which e-mail communications can be intercepted, it is likely that some measures to prevent interception by the parties to the communication should to be taken to ensure the communication is deemed to be confidential. Should legal practitioners or the courts fail to maintain the confidential nature of information they hold they may be in breach of any duty of confidence owed to the party providing the information.

2. Legal Professional Privilege.

The privacy of many communications between legal practitioners and clients, as well as any documents relating to a proceeding are also protected by the doctrine of legal professional privilege. The privilege covers a narrower field of information than a duty of confidence. Generally, communications for the sole purpose of legal advice and relating to a legal proceeding are protected from demands of disclosure with some limited exceptions.

Clearly, loss of legal privilege would be of significant detriment to anyone appearing before the court. A case may be severely undermined if, for example, communications between the solicitor and client which reveal the weaknesses of the parties position could be accessed by the opposing side and also tendered as evidence before the court. Increasing the likelihood that legal privilege may be lost, could result in a reluctance of clients to be frank with their legal representatives and thus affect access and the effectiveness of the legal system.

Legal professional privilege only extends to the protection of confidential information. As argued in the discussion on confidentially, it is likely that communication of information via unprotected e-mail, or otherwise unprotected information, would be inconsistent with any later claim that the information was of a confidential nature. While the law in the area is uncertain, clearly it would be prudent to ensure that a reasonable standard of security and privacy was adopted by legal practitioners to ensure legal privilege of client information.

3. Negligence.

Legal practitioners, having a clear duty of care in relation to acting in the best interests of their client, may also be liable for damage resulting from any loss of

privilege or confidentiality arising from their negligent conduct. It is even possible that a failure to take reasonable security measures may be held by the courts to constitute negligent conduct. When assessing whether an allegation of negligence is made out, courts will take into account current industry practice. Clearly, increased use and availability of precautionary measures in relation to the handling of sensitive information would make it increasing difficult to sustain an argument that non-adoption of reasonable precautions was not in breach of duty.

4. The Privacy Act.

The privacy of individuals is also protected in some respects by the Privacy Act 1988 (Cth). This Act imposes legal requirements concerning the handling of information. However, at present its application is limited to the regulation of the Commonwealth government and its agencies, credit providers and handlers of tax file numbers.

3. Proposed Standards of Security and Privacy.

A significant deficiency in the current privacy law framework is its general failure to regulate the conduct of those in the private sector who hold personal data. Moves to extend the law in this respect are fuelled by a growing concern in an increase in data matching practices of private companies. As well, a growing number of countries are adopting the guidelines of the OECD in relation to data protection. These guidelines regulate the conduct of both the public and the private sector and prohibit the transfer of information to other countries where standards of privacy are inadequate.

In February 1998 the Federal Privacy Commissioner released a recommended approach to the issue of information handling. The report outlines a set of National Principles which are in line with international standards and designed to assist the private sector in the development of their own, voluntary privacy codes.

In July 1998 the Victorian government released a proposal for the development of a Data Protection Bill. This Bill would be based on the National Principles. The aim of the proposed legislation would be to provide a minimum standard in relation to the handling of personal information by both the public and private sector within Victoria. The regime would also facilitate the development of industry based voluntary codes, which once approved would regulate the practice of the particular industry.

A Data Protection Bill is due to be released and introduced into parliament in the Autumn Session, 1999.

Of particular relevance to the issue of the protection of information from unauthorised access is Principle 4.1 which states that:-

"An organisation should take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure."

In addition, the storage of information would be regulated by Principle 4.2:-

"An organisation should take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose."

In a manner similar to the current legal requirements, these provisions would require information to be protected at a reasonable standard. Significantly, however, these requirements apply to the protection of any 'personal information' rather than being restricted only to confidential information. It must be noted, however, that the requirement of the National Principles only apply to information of natural persons and therefore the business information of a company would not be covered. Any breach of the proposed Victorian legislation would be open to investigation by the Privacy Commissioner, however any determination of the Commissioner is not of a binding nature. As such, the privacy provisions may lack a degree of force.

It is submitted that Principle 4.2 requirements would be satisfied by current storage procedures. Currently, the Legal Practice Act 1996 (Vic) s 443(1) allows a legal practitioner to destroy old client documents and information after seven years. This length of time is considered reasonably necessary so as to ensure that any possible litigation in relation to documents will be statute barred.

4. Summary - Sufficiency of the current legal framework to ensure adequate standards of security and privacy

It is apparent from the above survey of current and proposed law, that there is a requirement for the courts and legal practitioners to ensure a reasonable standard of security and privacy are maintained in relation to electronic information.

Any confidential information held by the courts or legal practitioners is protected from disclosure by a combination of a general law duty of

confidence and legal professional privilege. In order to ensure that a duty of confidence is not breached, those holding confidential information likely to be required to ensure reasonable levels of security are maintained. Failure to do so may give rise to actions in breach of confidence and negligence.

The proposed Data Protection Bill, will extend this protection to 'personal information'. It will also offer an alternative means of investigating alleged breaches of privacy standards.

Given the sufficiency of the requirements at general law and under the proposed Data Protection legislation there may be little need for the legal profession to draw up an industry specific code of practice in relation to the handling of sensitive information.

Yet two important questions remain. The first is the question of what is likely to constitute a 'reasonable' level of protection. The second, and more important questions, is whether this standard is sufficient to satisfy any concerns in relation to security and privacy so as to enable the legal system to utilise technological advances.

4. ***Prevention of Unauthorised Access and Use.***

The standard of security required by the holders of personal information is not stated in the National Principles or the Victorian legislative proposal. This approach is a deliberate attempt to ensure that the law is able to keep up with the rapid developments in methods for protecting data. Any common law requirement of protection is similarly not defined.

Thus, the level of protection from unauthorised access will depend on what is considered 'reasonable' given the possible methods for protection available at the time. Current methods of protection are outlined below.

1. Transmission of Information.

Protection of electronic communications is able to be ensured using specifically designed software systems. Currently, one of the simplest methods to prevent interception of electronic communications is to use some form of encryption. This involves an alteration of the transmitted message so that it can only be read by the intended parties. There are two primary methods of encryption.

The private key (also called secret key or symmetric) method involves one key or password, which is used to encrypt and decrypt the message. This method requires some prior communication between the parties in which the key has been privately exchanged. The level of protection this method offers

increases with the number of digits used in the key as this increases the number of digit combinations possible.

Public key (also called symmetric) systems involves the use of two keys, a public and a private. A user makes their public key generally known. Anyone wishing to send a message to the user can encrypt it using this public key. The message can only be decrypted by the corresponding private key, known only to the user. The user can encrypt a reply by using the public key of the other party. A public key system will be required to encrypt communications between parties who have never been in prior contact.

An effective public key system also requires some means of ensuring that the public key is actually that of the user, not someone merely using their name. This role can be performed by ‘certification authorities’, or ‘trusted third parties’ which conduct identification checks and provide certification of the level of investigation satisfied. Whether the regulation of the conduct of the certification authorities themselves should be left to private market forces or involve some government regulation is currently under consideration in Australia. Both the Commonwealth and Victorian government are inquiring into the prospect of establishing bodies which would recognise certification authorities who operated according to a particular standard.

In addition, to ensure that information is not disclosed to unauthorised persons, acting as an impostor and receiving the information directed to the recipient, there is an emerging global practice in the use of digital signatures. Digital signature technology applies mathematical algorithms to the text of a document, allowing a user to create a unique signature for the document. As the text of the document is used to create the signature, any subsequent alteration of the text will be easily detected an drawn to the attention of the recipient of the communication. Digital signatures potentially offer a greater degree of authentication than a hand-written signature and give greater guarantees that the document has not been tampered with after signing.

Digital signatures can be appended to communications using a public key system. Some systems allow this function to be combined with the encryption of the communication. The private key of the sender is used to generate the signature and the signature is checked by the recipient using the senders public key. Again, trusted third parties are needed to ensure that the particular signature truly belongs to a person.

It is also possible to created digital company seals by assigning each director a portion of the company's private key. Where a signed document needs to be witnessed, it is possible for the witness to attach their digital signature to a document already digitally signed.

2. Storage of Information.

Any computer system of the court or of a legal firm will need to be protected from unauthorised users as well as from loss or damage due to things such as computer viruses. Some required precautions may include the use of up-to-date anti-viral software, the back up of files, physical measures restricting the access of unauthorised persons to areas in the office, and ensuring password secrecy. It may also include use of encryption as discussed above.

As well, it may be necessary to develop a system to enforce a security policy between the network of the organisation and the public Internet. Such a system is known as a firewall. It determines which computers within the organisation may be accessed from the outside and which outside services may be accessed by those within the organisation. The actual system used by an organisation will need to be determined taking into account factors such as the level of protection required and the cost of setting up and running types of firewalls.

3. Current Practice

The Victorian government is in the process of introducing legislation to facilitate the use of public key technology. The relevant changes required to give digital signatures an equivalent legal status to traditional signatures is addressed in the Electronic Commerce Framework Bill 1998 (Vic). This Bill is in line with both international and Commonwealth developments in the area.

In addition the Bill will establish a trusted third party called the Electronic Signature Recognition Board. This board would authorise any private certification authorities meeting management standards and as such, further ensuring the authenticity of any digital signature and security for encryption technology.

Currently, there are a wide variety of encryption programs which provide a high level of security and are relatively easy to operate. Many are available as shareware. However as the available software is in a constant state of development, it is important that enquiries are made at the time of purchase as to the merits of particular programs and that any encryption program continues to be updated in the light of technological developments.

Many of the larger law firms in both Australia and abroad are beginning to use encryption technology as part of a firm security policy. The Law Institute in Australia has not developed, and is currently not working on, a set of guidelines to assist smaller practitioners in developing a data protection policy. However, the issue is often covered in local legal practice journals. Firm security policies also include the development of security mechanisms in order to ensure the protection of stored data. The use of anti-viral programs is becoming more and more widespread. Again, information concerning security mechanisms is available in legal practice journals as well as more general business and computing journals.

The court system is yet to engage in extensive electronic communications. Most of their trials have been conducted over LANs, between previously identified parties and therefore have raised few security problems. However, there has been a shift to usage of public networks, the Internet, by the Magistrates' Court and the Victorian Civil and Administrative Appeals Tribunal. As a result of security concerns, the adoption of electronic communication technology has been rather cautious. However as its use becomes more widespread, the corresponding security issues raised are being investigated and resolved.

5. ***Conclusions - Sufficiency of current technology to ensure confidence in an e-filing system.***

Initially it may be possible to restrict electronic information transmission to communications between the court and legal practitioners. As such, it may be possible to use a private key system, by which all Victorian legal practitioners would be issued with a private key by the court. This would eliminate the need to utilise trusted third party's and reduce risk of interception to a minimum.

However, should more general access to the court system by electronic means be desired then it may become necessary to utilise a public key system allowing digital signature and encryption technology to be used. As trusted third parties may perform differing levels of inquiry as to the identity of individuals requesting the issue of a public and private key, it will be important for the courts and legal profession to decide upon the level of inquiry which will be sufficient in order to satisfy any security concerns. It is likely that trusted third parties which have been authorised by the proposed Victorian Electronic Signature Recognition Board will be of a sufficiently high standard to meet the requirements of the profession.

While it may not be necessary to develop a specific code of practice in relation to the privacy of information given in a legal context, it may be desirable for the profession to set up some method of informing practitioners of the latest technology in the area of security. This is because of the often rapid developments of technology in the security and privacy area, and the wide variety of security measures which could and should be adopted by individual practitioners. This may be especially useful for smaller practitioners with less

resources from which to draw when designing security procedures for their computer systems.

In general terms, it does appear that the standard of security and privacy required in handling sensitive information and the level of protection offered by commonly available security programmes is of a sufficiently high standard to eliminate many of the risks inherent in the transmission and storage of electronic information. Provided that the security procedures are keep up to date, that passwords kept secret, and that the Victorian government does establish its signature recognition board, one may even contend that the usage of electronic technology in the legal process would provide a greater level of security than is currently offered by papers documents held together by a small staple and authenticated by a forgeable, handwritten signature.

3. Privacy — Anonymity and Electronic Law Reporting.

1. The Principle of Open Courts and Anonymity

The importance of the principle of an open and public judicial system is well established in our legal system. At common law, publicity of the courts is protected in all but the most exceptional circumstances. The principle of public justice includes not only the holding of proceedings in open court, but the corollary entitlement of those present to fairly and accurately report the proceedings.

An open legal system is generally considered to be justified as in the public interest. More specifically, it is argued that an open court is imperative as a democratic check on judicial power and in ensuring public confidence in the administration of justice. As well, publication of judicial decisions is fundamental in public knowledge of the law and in the ability to participate in any law reform. There is also argued to be a type of public propriety interest in the proceedings of the legal system, which is State funded and thus within the public domain. An open judicial system also preserves to some extent rights of freedom of speech, freedom of the press and the public's right to know relevant information, such as the criminal record, of people with whom they may have dealings.

Clearly, publication of a persons involvement in legal proceedings and information revealed in the course of the proceedings, may have negative consequences for that person including a damaged reputation. While these consequences are often recognised, in general they have been considered to be superseded by the importance of retaining judicial openness. This is especially the case in criminal proceedings, perhaps due to the State involvement in the proceedings or in a conception that a criminal reduces their right to privacy upon commission of a crime. In other areas of law, such as in civil disputes, family law matters, cases involving children or in proceedings

involving sex offences, the need to protect the individuals concerned in the matter has received a greater recognition at law. The issue has also arisen in the context of pre-trial publication of the identity of those charge with criminal offences. Another area in which concerns are raised is in the publication of details of sexual preference and HIV/AIDS.

2. The Current Law

In order to protect the openness of court proceedings, at common law there are only few exceptions to the rule that proceedings must be held in open court, such as where it would defeat the object of the action, prejudice the administration of justice or jeopardise national security. Where proceedings are held in open court the balance of authority suggests that there is no common law power for the court to prohibit publication of any of the proceedings.

This rule is amended by statute in all jurisdictions. In Victoria, the Supreme Court Act 1986 (Vic) s 18, 19 allow the court to prohibit publication of the whole or part of a proceeding where in the opinion of the court publication would endanger national security, prejudice the administration of justice, endanger the safety of a person, offend public decency or morality or cause undue distress to the complainant in cases involving sexual offences. The County Court Act 1958 (Vic) s 80 confers a greater level of discretion to the judges to prohibit publication of proceedings which in its opinion ought not be published. A more extreme alteration to the common law rule is found in relation to the Magistrates' Court of which no proceedings are reported. Similar provisions exist in other jurisdictions. In general, these provisions have rarely been used. Where they have, it has generally been to prohibit publication before judgment by the media rather than in relation to law reports.

Further, the National Principles for the Fair Handling of Personal Information require that personal information should only be disclosed where it is consistent with the expectations of the person or is in the public interest. This provision would not directly effect publication of law reports which are generally classified by the courts as in the public interest and would also be likely to be a reasonable expectation of people involved in litigation. However the Principles do demonstrate a growing recognition at law of the importance of individual privacy which ought to be borne in mind when considering the traditional approach to the publication of information revealed in the course of legal proceedings.

3. Electronic Reporting.

The current laws relating to suppression orders have developed in the context of a distinct system of law reporting. While publication of law reports has been carried out since as early as the eleventh century, recent years have seen a marked increase in the number of cases which are reported. Factors such as accessibility and interest, have kept circulation of law reports largely within the confines of those in law related professions. Media reporting brings the content of legal proceedings into wider public circulation, but even in this context it is only a small proportion of cases which receive widespread public attention.

The electronic publication of legal materials heralds a new era of accessibility and publicity of law reports. Where previously, a search for legal material was a specific task, now simple and general search engine query on a home computer may include in its results any relevant law report. The benefits of this accessibility are evident. Yet, electronic publishing also means that, at least potentially, a reported legal proceeding in which a person is involved can be retrieved with relative ease by any interested party along with information such as business details, sexual preference, medical history, and family disputes which may have been revealed in the course of litigation.

The scope of this report is limited to considerations of privacy in relation to electronic reporting. As such, it is beyond the terms of reference of this report to conduct a more general inquiry in the area, particularly in the debate which surrounds the ability of the media to publish pre-trial details of those charge with offences as well as the generally more restrictive circumstances in which the media may report legal proceedings. Rather, consideration is limited to whether the current practice of law reporting is in any way affected by a change from paper to electronic publication in the context of new privacy law regulations.

4. Possible Methods of Addressing any Privacy Concerns.

1. *Continue Current Practice*

It is possible to argue that the level of infringement of individual privacy involved in he electronic publication of law reports is not high enough to outweigh the benefits of openness and accessibility gained from electronic reporting. If this conclusion is made there may be little need to alter the present reporting procedures.

However, it may also be maintained that such a conclusion is not in line with the growing legal recognition of privacy rights. As such, there may be at

least some need to ensure that unnecessary personal and identifying information is omitted from law reports. Yet, it is arguable that current practice does offer sufficient means by which to ensure privacy is maintained. As well as limited provisions for the court to suppress publication of certain information, the body responsible for law reporting — the Council of Law Reporting — operate under a self-imposed standard by which they refrain from publishing unnecessary personal information.

2. ***Increase the Judicial Discretion to prohibit***

It may also be possible to address privacy concerns which may arise in the context of electronic reporting by attaching a legislative direction within the current legislation governing suppression orders so as to require judges to take into account arguments of damage to reputation.

However, it must be noted that reputation is a relative concept. Consideration of reputation when deciding whether to omit information from a law report has the potential to lead to inequality before the law. This is because professionals may be more easily able to identify tangible damage to their business and careers, which may ensue from the general release of certain information.

In addition, it is possible that promoting a higher level of judicial discretion in the area may lead to a non-uniformity of outcome. In addition, since one of the suggested rationales of the principle of court openness is to ensure judicial accountability, it may be inconsistent to then place the responsibility for defining the boundaries of openness upon the judges. In this respect, one should consider a recent decision of the NZ High Court in which a suppression order was made. The failure of the Court in this instance to deliver reasons of the suppression order highlighted the potential of a wide judicial discretion to suppress publication to undermine notions of openness and accountability of the judiciary.

3. ***Statutory expansion of categories of cases in which a restriction on publication may be allowed.***

In order to both ensure increased suppression of identifying information and to attempt to reduce judicial discretion in the area it may be desirable to place the matter in the hands of the legislature. Thus, specific

legislation regulating the suppression of certain information could be introduced. This approach is already practiced to a certain extent, for example in relation to proceedings involving children. In the light of electronic publication it may be desirable to extend the categories of information protected, for example in relation to sexuality or medical information.

4. ***All cases unpublished/ published without identifying people involved.***

While lower courts may not require proceedings to be published, it is unlikely that a similar practice would be considered appropriate for higher courts. It may, however, be possible to argue for the systematic removal of any identifying information in the law reports of courts at all levels. The greater suppression of personal information which would result, may be viewed as inconsequential since it can be argued that the real information of public interest is the procedures of the court, the decisions and the actions of judges. None of this information depend upon knowing the identity of the actual parties.

However, one should note a possible long term consequence of such a measure may be its effect of the current style of professional legal reasoning and argument. It is possible the suppression of factual information may shift the legal focus from the traditional fact orientation of the common law to a more principle oriented approach similar to Civil law systems.

5. Conclusion

Unfortunately, it is not possible to make definite recommendation as to the approach which should be adopted in relation to the protection of privacy in the context of law reporting. This is because of the limited scope of the current investigation. Since, issues relating to suppression orders have a great impact in relation to the regulation of media publication of pre-trial information, it would be undesirable to draw any conclusions without in depth consideration of this area.

However, was is clear from the current investigation, is that new technology developments do provide new factor in arguments relative to the publication of legal materials. The impact of technology on issues of privacy is of enough significance to justify a new, more in depth inquiry into the issue of suppression orders.

BIBLIOGRAPHY

ARTICLES AND BOOKS

Australian Privacy, *Everything You Always Wanted To Know About Digital Signature But Were Afraid To Ask* (1997). Available at http;//www.privacy.com.au/digsig1.htm

J H Baker, *An Introduction to English Legal History* (3rd ed) (1990: Butterworths, London)

Blackstone, *Commentaries on the Laws of England* vol 3 (1768) 373.

Stephen Colbran et al, *Civil Procedure: Commentary and Materials* (1998: Butterworths, Sydney)

Evatt, 'Family Law' in The Australian Press Council, *To Name or Not To Name* (1980: The Australian Press Council, Sydney)

Susan Friewald, 'Uncertain Privacy: Communication Attributes After the Digital Telephony Act' (1996) 69 *S Cal LR* 949.

Michael Froomkin, 'The Essential Role of Trusted Third Parties in Electronic Commerce; (1996) 76 *Oregon LR* 49

Robert L Jones, *Client Confidentiality: A Lawyer's Duties With Regard to Internet E-Mail*, (August, 1995) http://www.gsu.edu/%7Elawppw/lawand.papers/bjones.html.

Ian D Leader-Elliott, 'Legislation Comment: Suppression Orders in South Australia: The Legislature Steps In' (1990) 14 *CrimLJ* 86.

Ian J Lloyd, 'Detecting and Prosecuting Computer Crime', *Information Technology Law*, 186- 196.

Morag McDowell, 'The Principle of Open Justice in a Civil Context' (1995) *NZLR* 214.

Meagher, Gummow and Lehane, *Equity Doctrines and Remedies* (3rd ed) (1992: Butterworths, Sydney).

Scott Optican, 'Secret Law' (1997) *NZLJ* 77.

Rick Sarre, 'HIV/AIDS and Suppression Orders' (1995) 17(3) *Law Society Bulletin of SA* 11

Geoffrey Sawer 'Privilege' in the Australian Press Council, *To Name or Not To Name* (1980: The Australian Press Council, Sydney)

Chuck Semeria *Internet Firewalls and Security: A Technology Overview.* Available at http://www.3com.com/nsc/500619.html

Greg Taylor 'No guarantee' in The Australian Press Council, *To Name or Not To Name* (1980: The Australian Press Council, Sydney)

Lex Watson 'Discrimination' in Australian Press Council, *To Name or Not To Name* (1980: The Australian Press Council, Sydney)

REPORTS

Department of State Development, *Discussion Paper: Promoting Electronic Business: The Electronic Commerce Framework Bill* (July 1998, State Government of Vic).

Department of State Development, *Discussion Paper: Information Privacy in Victoria: Data Protection Bill* (July 1998)

Electronic Commerce Expert Group to the Attorney-General, *Report of the Electronic Commerce Expert Group to the Attorney-General* (31 March, 1988). Available at http://law.gov.au/aghome/advisory/eceg/single.htm

Law Commission of New Zealand, *Report 50: Electronic Commerce Part I: A Guide for the Legal and Business Community* (October 1998, Wellington)

OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980)

Privacy Commissioner, *National Principles for the Fair Handling of Personal Information* (February, 1998)

Standards Australia, *Strategies for the Implementation of a Public Key Authentication Framework (PKAF) in Australia* (1996), Project Gatekeeper

United Nations Commission on International Trade Law, Model Law 1996. Available at http://www.un.org.at/uncitral/texts/electcom/ml-ec.htm

CASES.

A-G v Observer Ltd [1990] 1 AC 109.

Attorney-General (NSW) v Mayas Pty Ltd (1988) 14 NSWLR 342.

Baker v Campbell (1983) 153 CLR 52.

Coco v AN Clark (Engineers) Ltd [1967] 2 All ER 415.

Commonwealth v Fairfax (1980) 147 CLR 39.

Edwards v Bardwell 632 F Supp 584 (MD La 1986).

Francome v Mirror Group Newspapers Ltd [1984] 1 WLR 892.

Jaench v Coffey (1984) CLR 549.

John Fairfax Group Pty Ltd (Receivers & Managers Appointed) and Anor v Local Court of NSW & Ors (1992) 26 NSWLR 131

Malone v Metropolitan Police Commissioner [1979] Ch 344

R v Cox and Railton (1884) 14 QBD 153.

Raybos Australia Pty Ltd and Anor v Jones (1985) 2 NSWLR 47

Re E and Australian Red Cross Society, Australian Red Cross Society NSW Div and Central Sydney Area Health Service (1991) 99 ALR 601

Rogers v Whitaker (1991) Aust Torts Reps 81-113

Scott v Scott [1913] AC 417.

Seager v Copydex Ltd (No 1) 2 All ER 415

Victoria Park Racing and Recreation Grounds Co Ltd v Taylor (1937) 58 CLR 479.

LEGISLATION.

Children and Young Persons Act 1989 (Vic).

County Court Act 1958 (Vic)

Crimes (Computers) Act 1988 (Vic)

Crimes Act 1914 (Cth)

Family Law Act 1975 (Cth)

Judicial Proceedings Reports Act 1958 (Vic)

Legal Practice Act 1996 (Vic)

Limitation of Actions Act 1958 (Vic)

Magistrates' (Summary Proceedings) Act 1975 (Vic)

Privacy Act 1988 (Cth)

Summary Offences Act 1966 (Vic)

Supreme Court Act 1986 (Vic)

Telecommunications (Interception) Act 1979 (Cth)