

4 June 2007

The Executive Director
Australian Law Reform Commission
GPO Box 3708
SYDNEY NSW 2001
privilege@alrc.gov.au

Seamus E. Byrne

[REDACTED]

1. AUTHOR

- 1.1. This submission has been prepared by Seamus E. Byrne, Lawyer and Director of Forensic Technology with Vincents Chartered Accountants.
- 1.2. Seamus has extensive experience in the legal issues associated with the exercise of coercive information-gathering powers by Federal Investigatory Bodies (**FIBs**).
- 1.3. His professional biography is located at: <http://www.seamusbyrne.com>.

2. EXECUTIV E SUMMARY

- 2.1. This submission addresses select questions¹ raised by the Issues Paper in relation to FIBs, legal practitioners and their clients in managing claims of client legal privilege (**privilege**)² in ESI.
- 2.2. This submission is brief due to time constraints and it is anticipated that a more detailed response will be provided to the forthcoming Discussion Paper in August 2007.

¹ Questions 5-1(b) and 5.5.

² Also commonly referred to as legal professional privilege.

3. SUBMISSIONS TO SPECIFIC QUESTIONS

3.1. Question 5-1(b): “*What problems arise concerning - In particular, where information the subject of a potential claim for privilege is held in electronic form or is sought to be seized during the execution of a search?*”

Led by the adoption of computers and associated technologies, it is submitted that client legal privilege (**privilege**) in electronically stored information (**ESI**) is the most significant issue faced by those within Federal Investigatory Bodies (**FIBs**) who endeavour to dutifully exercise their coercive information-gathering powers and the legal practitioners who must represent their client and efficiently deal with privilege issues.

Search and Seizure of Electronically Stored Information (ESI)

It is recommended that ESI, as potential electronic evidence, should be searched and seized by FIBs with the use of specialist computer forensic personnel.³ It is submitted that while technology itself cannot resolve the issues pertaining to privilege, recent advances, such as logical forensic imaging and live forensics, provide greater flexibility in the search and seizure of ESI.

Traditional computer forensics usually involves ‘pulling the plug’ to shut down the computer, previewing the one or more hard drives contained within the computer for relevance (e.g. by searching for keywords which pertain to the search warrant), creating a forensic image (or exact copy) of the one or more hard drives contained within the computer onto another hard drive or optical storage (e.g. CD/DVD) (**physical forensic imaging**).⁴

An emerging practice in the specialised field of computer forensics provides the opportunity to seize selected ‘active files’⁵ stored on a hard drive or other electronic storage media by creating a forensically-acceptable image (or copy) of specified files (**logical forensic imaging**). For example, a logical forensic image of all active Microsoft Word documents within a certain key custodian’s directory on a corporate server. Alternatively, a logical forensic image may be created of all active electronic files on a hard drive returned from a keyword search. It is submitted that logical forensic imaging may be a feasible alternative in non-hostile situations⁶ when the FIB is absolutely positive that only a specific amount of active

³ FIBs either utilise their internal computer forensic resources, engage outside assistance from another Government Department, the Australian Federal Police (**AFP**) or an outside entity to assist in the search and seizure of ESI.

⁴ This process was outlined, at a high level, in: *Kennedy v Baker* [2004] FCA 562 [24-27].

Alternatively, one (1) or more hard drives may be imaged first and then searched to ascertain relevance.

⁵ The term ‘active’ is used to contrast with ‘deleted’ or otherwise inaccessible data which may be interpreted as information on a hard drive or other electronic storage media.

⁶ In contrast to hostile situations such as those apparent in: *Prescience Communications Limited v Commissioner of Taxation Office* [2006] FCA 1561 [10].

electronic files on a hard drive need to be seized, as opposed to an entire hard drive which may take substantially longer to create a forensic image of, and may give rise to claims of privilege.

An additional emerging practice is to create a forensically-acceptable forensic image whilst a computer is still in operation (**live forensics**). This method, as opposed to traditional computer forensics, allows for ESI contained on one or more computers on a computer network to be searched for relevance and seized with minimal disruption to the operations of the computers involved.⁷

To date, only a very small number of computer forensic specialists within Australian FIBs have had relevant training and experience in both logical forensic imaging and live forensic methods to seize ESI. It is submitted that increased adoption of such technology is an important step in avoiding situations such as those described in *JMA Accounting*⁸ where, *inter alia*, the operations of an accounting practice were disrupted for two (2) full days while physical forensic imaging was performed.

Identifying, Raising and Resolving Claims of Privilege in Electronically Stored Information (ESI)

Four (4) issues continue to arise in relation to privilege and ESI, namely:

- (a) What constitutes a claim of privilege in ESI;
- (b) The method by which privilege claims are to be identified;
- (c) The method by which privilege claims are to be raised; and
- (d) The method by which privilege claims are to be managed and agreed to between the FIB and involved parties.

Issues (c) and (d) are arguably dealt with by **[Question 5-5]**.

Issue A

Case law currently provides that privilege will generally be maintained following the creation of a forensic image and removal from the search premises.⁹ It is also acknowledged that privilege attaches to, and protects confidential communications as information, and not documents as such.

This issue is compounded by the fact that privileged information in ESI may be contained not only in active and readily accessible electronic files, but may also be present on a hard drive or other electronic

⁷ It also must be noted that 'live forensics' may also assist in situations where ESI is required to be seized covertly or for the seizure of encrypted ESI.

⁸ *JMA Accounting Pty Ltd v Commissioner of Taxation* [2004] FCAFC 274.

⁹ *Kennedy v Baker (No 2)* (2004) 138 FCR 414 [16];

JMA Accounting Pty Ltd v Commissioner of Taxation [2004] FCAFC 274 [23].

Prescience Communications Limited v Commissioner of Taxation Office [2006] FCA 1561 [31].

storage media, albeit, in a deleted form.¹⁰ It is submitted that it is currently unclear as to whether a diligent legal practitioner can and/or should make a claim in privileged information which, for all intensive purposes isn't readily accessible by their client, but is likely accessible by FIBs with use of their specialist computer forensics personnel.

From a legal perspective, it is arguable whether privilege would be waived due to uncertainty as to how the '*inconsistency test*'¹¹ would be applied to interpret such a claim under the circumstances, or whether the information would continue to be protected under inadvertent disclosure or another related exception. It is submitted that this is an issue that must be resolved with priority to reduce privilege being used a weapon to stall the efforts of investigations and litigation alike.

It is further submitted that the recent comments of Will Irving, In-House Counsel for Telstra Corporation "*calling for tough sanctions against clients who claim privilege where none exists and the lawyers who advise them to do so*" is most definitely a step in the right direction.¹² However, such sanctions must only be implemented when privilege is clearly defined.

Issue B

It is submitted that the practicalities of identifying privilege in ESI present an entirely distinct problem from hard-copy (paper) information regardless of whether seized by FIBs or during the process of discovery¹³ as part of civil litigation.

Recent case law illustrates the ever-increasing problems faced by legal practitioners and their clients in identifying privileged information in ESI. This is due to the much larger volume of information for review¹⁴ and the various formats in which privileged information may be stored in ESI. It is submitted legal practitioners should force appropriate information management as a proactive consideration for clients prone to the attention of FIBs and seriously consider consulting specialist advisory to assist in the expeditious filtering and identification of privileged information.

¹⁰ It is readily acknowledged that deleted electronic files, as data, are generally recoverable by a computer forensic specialist unless securely deleted or overwritten.

¹¹ As outlined in *Mann v Carnell* (1999) 201 CLR 1 [13] per Gleeson CJ, Gaudron, Gummow and Callinan JJ. Notably supported in *AWB Limited v Honourable Terence Rhoderic Hudson Cole (No 5)* [2006] FCA 1234 [131].

¹² Author Unknown, 'Irving urges privilege crackdown' (2007) 45(4) *Law Society Journal* 30.

¹³ Also referred to as disclosure in Queensland, South Australia and the United Kingdom.

¹⁴ *Kennedy v Baker* [2004] FCA 562 [103];

Oke v Commissioner of Australian Federal Police [2005] FCA 1363 [18], [32].

3.2 Question 5-5: “Do policies and procedures governing the execution of Commonwealth search warrants need to be amended specifically to address claims made for privilege in respect of documents stored electronically?”

It is submitted that FIBs will continue to face blanket claims of privilege and undesirable outcomes to their investigations unless current policies and procedures are revised to provide clear processes for dealing with claims of privilege in ESI.¹⁵ Such policies and procedures must be publicly documented, practicable and consistently followed by warrant holders.¹⁶ The ideal outcome is for guidelines that facilitate claims of privilege in ESI to be raised, identified and resolved in a timely manner.

¹⁵ As a pertinent example, *Oke* was a flawed search warrant execution for many reasons and arguably highlights apparent issues related to the practical knowledge of warrant holders and legal practitioners alike in dealing with claims of privilege in ESI: *Oke v Commissioner of the Australian Federal Police* [2007] FCA 27.

¹⁶ The Australian Taxation Office (ATO) ‘*Access and Information Gathering Manual*’ is the best effort to date. Chapters 5 and 6 refer to Electronically Stored Information and Privilege respectively. However, *Prescience* demonstrates that even with policy and procedure, the ATO still encounters issues in executing, and agreeing to, protocols which adequately manage claims of privilege.