

5 November 2007

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

Seamus E. Byrne

[REDACTED]

Geoffrey James Minchin Lambert
Director, Forensic
KordaMentha
GPO Box 2985
MELBOURNE VIC 3001
glambert@kordamentha.com

1.0 AUT HORS

- 1.1. This submission has been jointly prepared by Seamus E. Byrne¹ and Geoffrey Lambert.²
- 1.2. The authors are Australian legal practitioners with extensive experience in the operational and legal issues associated with the exercise of coercive information-gathering powers by Federal Investigatory Bodies (**FIBs**).
- 1.3. In addition to their experience in planning, executing and managing the coercive information-gathering powers of FIBs, the authors recently published an article on the harmonised Search (Anton Piller) Orders practice guidelines.³

¹ LL.B, CISSP, CCE, EnCE. Professional biography located at: <http://www.seamusbyrne.com>.

² LL.B, GCLP. Prior to commencing with KordaMentha in October 2007, Geoffrey facilitated the computer forensic and electronic evidence management capabilities within the Australian Competition and Consumer Commission (**ACCC**) and the Australian Taxation Office (**ATO**).

³ Seamus E. Byrne and Geoffrey Lambert, 'Practice Direction Update: Search (Anton Piller) Orders in Queensland' (2007) 27(9) *Proctor*, 17-19.

2.0 EXECUTIVE SUMMARY

- 2.1. This submission addresses select proposals⁴ raised by the Discussion Paper in relation to FIBs, legal practitioners and their clients in managing claims of client legal privilege (**privilege**)⁵ in respect of electronically stored information (**ESI**).
- 2.2. It is recommended that this submission be read in conjunction with Byrne's submission to Issues Paper 33.⁶
- 2.3. A forthcoming paper by Byrne and Lambert, 'Privilege, ESI and Information-Gathering Powers', will comprehensively address the increasing range of theoretical and practical issues in this area.⁷ It will also provide detailed strategies and procedures for resolving privilege issues involving ESI in relation to a broad range of specific powers.

3.0 SUBMISSIONS TO SPECIFIC PROPOSALS

- 3.1. **Proposal 8-16:** *"Federal client legal privilege legislation should provide that where information which may be subject to a claim for client legal privilege is stored on the same electronic medium as non-privileged information that falls within the scope of a Commonwealth search warrant:
(a) the executing officer is not precluded from copying or imaging that medium and causing it to be removed from the premises for further inspection; and
(b) such copying or imaging does not amount to a waiver of privilege."*

As a general principle, it is agreed that Federal privilege legislation should not preclude an executing officer of a search warrant from copying or imaging ESI and/or removing the copy or image from the premises for further inspection and examination. Further, consistent with current case law, it is agreed that the copying and/or imaging of ESI, which may be subject to a claim for privilege, does not amount to a waiver of privilege in otherwise lawful circumstances.

However, it must be appreciated that there are significant procedural differences between a Commonwealth search warrant⁸ and other coercive information-gathering powers. Fundamentally, a Commonwealth search warrant inherently provides search and seizure (i.e. removal) powers.⁹ In contrast, coercive information-gathering powers, such as those afforded to the ATO, are readily

⁴ Proposals 8-16, 8-17, 8-18.

⁵ Also commonly referred to as legal professional privilege.

⁶ Seamus Byrne, *Submission LPP 19*, 4 June 2007.

⁷ Based on an adapted May 2006 Research Paper by Lambert as part of Masters of Law (LL.M) studies at Monash University.

⁸ *Crimes Act 1914* (Cth) s 3E.

⁹ *Crimes Act 1914* (Cth) s 3F.

limited to the mere access to, and copying of, relevant information.¹⁰ This distinction requires diligent consideration as proposed Federal privilege legislation is drafted.

- 3.2. **Proposal 8-17:** “*The Law Council of Australia, the Australian Federal Police, the Commonwealth Director of Public Prosecutions, and relevant accounting professional bodies in consultation with:*
- (a) *federal bodies that possess search and seizure powers; and*
 - (b) *computer forensic experts,*
- should devise a set of guidelines to cover the resolution of client legal privilege claims in respect of electronically-stored information (The ESI Guidelines).*
- The ESI Guidelines should be adaptable for use at searches of premises of lawyers and accountants, other premises and searches of the person, and should be provided to persons at the time a Commonwealth search warrant is executed. The ESI Guidelines should, as far as possible, be consistent with the processes for dealing with the resolution of privilege claims in respect of information in paper form.”*

It is re-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 discovery.¹¹

This may be illustrated by the recent Supreme Court of Victoria case, *GT Corporation v Amare Safety*¹², where engaged consultants, as purported computer forensic experts for the applicant, provided a substantial volume (over 150,000 data files and thousands of electronic mail (e-mail) messages) in a disparate manner, without list or index.¹³ This resulted in the receiving party, and the Court, being unable to ascertain the custodian and/or source of the ESI. Further, the engaged consultants, did not appear to take any reasonable steps to remove documents, in which privilege would appear to be ordinarily claimed, from the document set provided for the purposes of discovery.¹⁴ In conclusion, Justice Hollingworth made the following assertion, “*I have no doubt that the manner in which [the applicant’s] electronic discovery was provided, together with the complete lack of any index, has contributed significantly to the problems which have subsequently arisen*”.¹⁵

¹⁰ *Income Tax Assessment Act 1936* (Cth) s 263.

¹¹ Seamus Byrne, *Submission LPP 19*, 4 June 2007, 4.

¹² *GT Corporation Pty Ltd v Amare Safety Pty Ltd* [2007] VSC 123.

¹³ *GT Corporation Pty Ltd v Amare Safety Pty Ltd* [2007] VSC 123, [36].

¹⁴ *Ibid* [37].

¹⁵ *Ibid* [36].

Client Legal Privilege and Federal Investigatory Bodies

ALRC Discussion Paper 73

Liaison between the Law Council of Australia (**LCA**), Australian Federal Police (**AFP**) and other relevant bodies is essential.¹⁶ It is strongly proposed that any ESI Guidelines should be developed with stakeholders referred to in **Proposal 8-17** and in conjunction with the meaningful input of experienced legal practitioners who possess demonstrated technical and practical working knowledge of ESI and the relevant legal framework. Such collaboration and endeavours will likely ensure that the proposed ESI Guidelines are able to be applied as consistently as possible with more traditional paper-based information.

The fundamental concern should be focused towards the Court receiving the best opportunity to be presented with the most appropriate and relevant information available. The appropriate preservation of the information in the first instance, and having that information placed with an independent third-party, under the authority of the Court is preferable.

As a high-level framework, the ESI Guidelines may exist in relative consistency with those applied to paper information, if appropriate safeguards are implemented in relation to the following concise preliminary procedure:¹⁷

1. The executing officer, with appropriate operational experience, and in consultation with an appropriately trained computer forensic expert, will make an appropriately information decision as to how data within the ambit of their coercive information-gathering power will be copied and/or imaged.
2. Data copied and/or imaged (**i.e. seized data**) is placed in the safe custody of the nearest mutually agreed-upon independent third-party (e.g. Supreme Court or Australian Government Solicitor office) for a preliminary fixed review and identify period (**review and identify period**), with the Claimant having access to an appropriate discretionary Court extension (e.g. up to 14 days).
3. The Claimant has the opportunity to review seized data and identify information subject to a claim for privilege. This may be conducted either using their own ESI and experts, or after obtaining a forensically-acceptable copy of the seized data from the FIB.
4. Privileged information is identified, appropriately listed and provided by the Claimant.¹⁸

¹⁶ Lambert, whilst at the ATO, liaised closely with the AFP in developing appropriate strategy and procedure to assist in the resolution of privilege claims in relation to ESI which were subsequently considered by both AFP Operational and Legal departments.

¹⁷ This preliminary procedure is to be considered a very concise draft.

¹⁸ It is anticipated that the compilation of such a list would be prepared electronically.

Client Legal Privilege and Federal Investigatory Bodies

ALRC Discussion Paper 73

5. Following the resolution of privilege claims, information subject to privilege is to be excluded from inspection and/or examination. This may be undertaken utilising one of the following methods:¹⁹
 - (a) Where data (e.g. documents) are merely logically copied, privileged data is securely erased;
 - (b) Where a logical forensic image is taken, a further logical forensic image is created by excluding the privileged data; or
 - (c) Where a physical forensic image is taken, the physical forensic image is restored and privileged data, in active and/or deleted form, is securely erased.²⁰
6. Alternatively, within the review and identify period, the Claimant has the opportunity to propose that the burden of ascertaining privilege is too great in comparison with time and cost reasonably likely to be incurred. In such cases, the Court may order that inspection and examination may proceed on a 'without prejudice' regard for privilege.²¹

It is also proposed that the ESI Guidelines address the educational requirements of the relevant FIBs and the legal profession. Such awareness will endeavour to facilitate an understanding of the multiple, and increasing methods, in which ESI may be copied and/or imaged for inspection and examination in a forensically-justifiable manner.

The proposed Federal privilege legislation must also provide appropriate safeguards which ensure that any data copying and/or imaging is undertaken in a manner proportionate to the nature of the investigation and the severity of operational disruption to be incurred by the entity under investigation.

¹⁹ Secure erasure would obviously alter the original seized data. Consequently, any alteration of the seized data is to be undertaken on a forensically-verifiable copy of the seized data. The original seized data is to remain at the agreed-upon independent third-party until Court-ordered destruction or the FIB communicates that the seized data is no longer required and is returned to the Claimant and/or securely destroyed.

²⁰ Alternatively, the methodology in (b) may be applied to the physical forensic image.

²¹ It is anticipated that this avenue would act similar to the case management directions in relation to discovery outlined in the Supreme Court of New South Wales Equity Division Practice Note 3 (Eq 3).

Client Legal Privilege and Federal Investigatory Bodies

ALRC Discussion Paper 73

- 3.3. **Proposal 8-18:** *“Federal bodies with coercive information-gathering powers—the exercise of which raise, or are likely to raise, the issue of the application of client legal privilege—should develop and publish policies and procedures in relation to managing and resolving claims for privilege in respect of electronically-stored information. The policies and procedures should, as far as possible, be consistent with the processes for dealing with the resolution of privilege claims in respect of information in paper form.”*

It is agreed that FIBs should take immediate steps to develop and make publicly available their policies and procedures in relation to managing and resolving claims for privilege in respect of ESI.

The need for the publicly available policies and procedures is essential to ensure transparency and provide an ‘important safeguard of rights’ to restore a balance where FIBs arguably possess increasingly broad coercive information-gathering powers and the resources to undertake such expansive investigations.