

Okay computer?



Recently revised Federal and Supreme Court practice guidelines recommend the engagement of an independent computer expert for search orders where computer searches are envisioned, **Seamus Byrne and Geoffrey Lambert** write

Search orders, also known as Anton Piller orders after *Anton Piller KG v Manufacturing Processes Ltd* [1976] Ch 55, are “designed to preserve important evidence” which may be relevant to an issue in an actual or anticipated proceeding: *Federal Court Rules* O 25B r 2. Search orders are generally granted and subsequently executed ex parte. Historically, such a remedy has most readily been exercised in matters relating to the infringement of intellectual property rights (IPR), such as copyright theft or unauthorised trademark usage: Mark Holler, “Anton Piller orders in Australia,” *Brief*, vol 32, no 9, 2005, 10–17.

In May 2006, the Federal Court of Australia published a revised Practice Note 24 for search orders. This article flows from the “harmonisation of court rules” project undertaken by the Council of the Chief Justices of Australia and New Zealand. Localised Australian jurisdictions have subsequently introduced harmonised practice guidelines (see box), which are notable, inter alia, for: extending the duties of the independent solicitor beyond mere supervision of search order execution; recommending the engagement of an independent computer expert (ICE) where computers may form part of a search; and providing clarity in dealing with claims of

privilege in relation to electronically stored information (ESI) as part of a search order.

The independent solicitor

The independent solicitor is a fundamental part of the search party and their role has been extended well beyond mere service and supervision of the execution of the search order: see *Microsoft Corporation v Goodview Electronics Pty Ltd* [1999] FCA 754.

According to the Federal Court of Australia’s Practice Note 24 (5 May 2006), the duties of the independent solicitor include: compiling a list of all things to be removed from the respondent’s premises; verifying the compiled list with the respondent for accuracy; taking custody of all things removed from the respondent’s premises until the return date (this ordinarily includes things that are disputed as within the scope of the order); submitting a written report to the Court regarding the execution of the order; and attending Court on the return date to potentially release things removed from the respondent’s premises.

Computers and the independent solicitor

The Practice Note specifies that the independent solicitor has discretionary power to “remove a computer from the premises for safekeeping or for the purpose of copying

its contents electronically or printing out information in documentary form”. It is submitted that this discretionary power should only apply where an ICE was not appointed as computers were clearly not envisaged as part of the search order.

The example search order in Practice Note 24 also provides that the independent solicitor will give undertakings to the Court, including specifying that the search order be executed in a manner “so as to minimise disruption to the respondent”. In addition to the high probability risk of evidence spoliation, a well-intentioned independent solicitor taking a respondent’s standalone computer system “offline” for a few hours or removing one or more computers can potentially result in significant unnecessary disruption. The ubiquity of computer networks creates even further risk in the event of well-intentioned access or removal of mission-critical computers.

Recent case law highlights the difficulties and consequences readily associated with obtaining and managing ESI: see *Metso Minerals (Australia) Ltd v Kalra* [2007] FCA 2108; *GT Corporation Pty Ltd v Amare Safety Pty Ltd* [2007] VSC 123; and *Oke v Commissioner of the Australian Federal Police* [2007] FCA 27. These recent changes impose a significant and as yet untested duty upon the independent solicitor and there is a clear need for these individuals to have or be provided the opportunity to obtain appropriate experience in dealing with electronic evidence. Alternatively, it is highly advisable to outsource such tasks to an ICE.

The independent computer expert

The ICE is increasingly seen as an essential member of the search party when computers are anticipated as part of a search order. However, the Federal Court Practice Note currently provides no guidance or clarification as to the qualifications and experience required for an individual to be appointed as an ICE. Notwithstanding, it is reasonable to assume that such individuals have a demonstrated understanding of, as well as operational and practical experience in, both the relevant law and technology.

This is essential to developing strategies to assist legal professionals identify, secure and manage ESI that falls within the scope of the relevant order as well as the subsequent analysis, management and presentation of such ESI as evidence before a court of law: see Eoghan Casey's *Digital Evidence and Computer Crime*, (2nd edn; Academic Press, 2004) and Standards Australia's *Guidelines for the Management of IT Evidence* (HB 171-2003) (2003).

In particular, according to Practice Note 24, the role of the ICE may include:

- (a) searching the respondent's computers for listed things in the form of ESI;
- (b) making a copy of one or more computer hard drives;

- (c) ensuring a chain of custody is maintained for each computer hard drive and copies thereof; and
- (d) producing a report as to the performance of their preliminary findings, generally including their search regime, a directory and file listing of ESI contained on the forensic images of the hard drives.

Consequently, an ICE should have a clear understanding of their role and a concomitant ability to act as a "technology translator" facilitating effective and meaningful outcomes for all relevant parties in terms of the relevant order.

Reasonable endeavours, minimal disruption and computers

Similar to the independent solicitor, the ICE must undertake to perform their duties with minimal disruption to the respondent. Traditional computer forensics typically involves shutting down or "pulling the plug" on a computer prior to creating a forensic image (also referred to as a "bit-stream copy") of the one or more physical hard drives within the computer (physical forensic imaging). But this is a broad generalisation and it is beyond

the scope of this article to discuss the various historical and current approaches available to a computer forensic practitioner.

Creating a forensic image of even a modern "average sized" computer hard drive can be time intensive. As mentioned above, this clearly has the potential to cause disruption to the respondent. Recent case law has permitted the ICE to remove a computer, in non-hostile environments, where additional time is required to create a physical forensic image: *Metso Minerals (Australia) Ltd v Kalra* (No 2) [2007] FCA 2108.

However, emerging computer forensics techniques, variously referred to as "live forensics", facilitate forensic imaging while the computer is still running and in operation – resulting in less, little or no downtime to the respondent's computer (and business operations which rely upon such computers). It must also be noted that some business and mission-critical computers cannot be turned off at all without significant risk of damage or data loss.

In addition, tools and strategies are available that facilitate "logical forensic imaging", that is, creating a forensically-acceptable image (or copy) of specified files outlined within a search order. For example,

(continued on p16)

Your documents are in safe hands

Docscorp

Compare any two documents with compareDocs
Even Word to PDF!

- PDF CREATION
- DOCUMENT ENCRYPTION
- PASSWORD PROTECTION
- PDF REDACTION
- SECURE EMAILS
- METADATA REMOVAL
- DIGITAL SIGNATURES

ph 02 8270 8500 www.docscorp.com e pdfdocs@docscorp.com

ACLA members can register online
www.docscorp.com/acla
to receive a complimentary copy of pdfDocs Desktop and compareDocs

(continued from p15)

the scope of what is forensically copied could be limited to all Microsoft Word documents within a specific user's folders or directory. Such techniques have idiosyncrasies with the potential to impact all parties which should ideally be understood by all parties and be considered and discussed at the earliest possible point in time.

Regardless of the strategy employed by the ICE, it is essential that the independent solicitor sufficiently understands such tools and strategies to both effectively supervise and discharge the duty imposed upon them. For example, the independent solicitor should ideally have a level of knowledge sufficient to inquire as to whether the methodology, tools and processes employed by the ICE are forensically acceptable, justified under the circumstances and within the scope of the ICE's expertise.

Computers and the respondent

Subject to the restrictions on entry, search and removal, the respondent must: disclose the location of "all computers, computer disks and electronic information storage devices"; provide all necessary passwords to access and operate computers; permit an ICE to search any computer and make a copy of any computer hard drive; and permit an ICE or the independent solicitor to remove any computer or computer hard drive.

From the time prior to admitting entry to the search party until the return date, according to the Practice Note the respondent also must "not disturb or remove any listed things". Due to the nature of ESI, it is highly likely that adverse consequences would follow if the respondent was found to have intentionally deleted, overwritten or otherwise destroyed "potentially relevant" ESI during this time.

Common law principles pertaining to document destruction were outlined in: *McCabe v British American Tobacco Australia Services Ltd* [2002] VSC 73; [2002] VSCA 197 (McCabe). Following *McCabe*, Victoria introduced the *Crimes (Document Destruction) Act 2006* and *Evidence (Document Unavailability) Act 2006*.

KEY POINTS

- Recently revised Federal and Supreme Court practice guidelines recommend the engagement of an independent computer expert (ICE) for search orders where computer searches are envisioned.
- Verify the qualifications and competency, both technical and legal, of an ICE.
- Know how to deal with privilege claims as part of a search order, including electronically stored information (ESI).

Dealing with claims of privilege

The Federal Court Practice Note sets out the following procedures, as a guideline for dealing with privilege claims as part of a search order:

Hardcopy documents

Prior to permitting entry to anyone other than the independent solicitor, the respondent has the opportunity to place any documents passed between the respondent and its lawyers subject to privilege to the independent solicitor to be sealed in an envelope or container. Anything provided via this method is not to be inspected by anyone until the return date.

Prior to the return date, the respondent shall be entitled, in the presence of the independent solicitor to inspect anything removed from the premises and make copies of the same, and provide the independent solicitor with a signed list of things which are claimed to be privileged or confidential.

On the return date, privilege claims are to be considered.

Computers and electronically stored information (ESI)

In regard to computers and ESI, the following process is applied:

The respondent is entitled to object to the conduct of the ICE on the ground that the computer contains material that is otherwise privileged. Upon the making of such an objection, the conduct of the ICE becomes inoperative to the extent of the objection. For example, the ICE may be prevented from searching and creating a forensic image of one or more computers.

If the respondent objects, and the applicant proposes to contest the objection, the role of the ICE is limited to removing the computer (or the computer hard drive) from the premises and delivering it into the custody of the independent solicitor for delivery to the Court at or prior to the return date.

If computers are left and only a forensic image is taken, the respondent should be able to provide a signed list of things claimed to be privileged or confidential on the computers. Or, if the computer or computers are taken prior to the return date, the respondent shall

be entitled, in the presence of the independent solicitor to inspect anything removed from the premises and make copies of the same, and provide the independent solicitor with a signed list of things which are claimed to be privileged or confidential.

On the return date, privilege claims are to be adjudicated.

The practice guidelines in practice

Recent case law, including that involving the Federal Court Practice Note, has highlighted the myriad of issues faced by lawyers when addressing strategies to identify, collect, search and manage large volumes of ESI: *Aristocrat Technologies Australia Pty Ltd v Global Gaming Supplies Pty Ltd* [2006] FCA 1707. The harmonised practice guidelines have arguably resulted in increased and timely judicial consideration of significant issues related to ESI.

This was also illustrated by recent commentary of the Australian Law Reform Commission, albeit from the coercive information-gathering perspective of specific Australian Government departments: *Privilege in Perspective: Client legal privilege in federal investigations*, Report 107 (2008) 8.332–8.375.

However, given the continued ubiquity of ESI, it is submitted that authoritative standards, guidelines, accreditations or qualifications regarding ICE's need to be considered and developed by relevant stakeholders, including the Law Council of Australia and Law Societies, to facilitate the informed engagement and verification of such individuals.

Further, the roles of the independent solicitor and the ICE need to be further developed to effectively address and manage privilege claims as part of a search order, particularly in relation to ESI. And appropriate general awareness and education strategies need to be developed by relevant stakeholders and delivered to those individuals involved in seeking and executing search orders with a view to formalising appropriate minimum requirements.

Seamus Byrne is chief operating officer at eDiscovery Tools. See www.seamusbyrne.com.

Geoffrey Lambert is director of forensics at KordaMentha.

This is an updated and revised version of an article first published in *Proctor*.

HARMONISED PRACTICE GUIDELINES

As at time of writing, the following Australian jurisdictions have introduced the harmonised practice guidelines:

- Supreme Court of New South Wales, Practice Note SC Gen 13 (14 June 2006)
- Supreme Court of Tasmania, Practice Direction 4/2006 (19 July 2006)
- Supreme Court of Victoria, Practice Note 2/2006 (1 September 2006)
- Supreme Court of South Australia, Practice Direction 4.3 (4 September 2006)
- Supreme Court of the Northern Territory, Practice Direction 6/2006 (27 November 2006)
- Supreme Court of Western Australia, Practice Direction 6/2007 (2 May 2007)