



Practice direction update:

Search (Anton Piller) orders in Queensland

Search orders are generally granted and subsequently executed *ex parte*.³ 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.⁴ Such orders are also known as Anton Piller orders.⁵

On May 8, 2007, the Supreme Court of Queensland published a revised practice direction for search orders.⁶ This update follows the continued “harmonisation of court rules” project undertaken by the Council of the Chief Justices of Australia and New Zealand and subsequent introduction of the revised Federal Court of Australia Practice Note in May 2006.⁷ These harmonised court rules are notable, *inter alia*, for:

(a) extending the duties of the independent solicitor beyond mere supervision of search order execution

(b) recommending the engagement of an independent computer expert (ICE) where computers may form part of a search, and

(c) providing clarity in dealing with claims of privilege in relation to electronically stored information (ESI) as part of a search order.

KEY POINTS

1. 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.
2. Verify the qualifications and competency, both technical and legal, of an ICE.
3. Know how to deal with privilege claims as part of a search order, including electronically stored information (ESI).

Article by Seamus E. Byrne¹ and Geoffrey Lambert²

The independent solicitor

The independent solicitor is a fundamental part of the search party⁸ and their role has been extended well beyond mere service and supervision of the execution of the search order. The duties of the independent solicitor include:⁹

(a) compiling a list of all things to be removed from the respondent’s premises

(b) verifying the compiled list with the respondent for accuracy

(c) 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 order¹⁰

(d) submitting a written report to the court regarding the execution of the order, and

(e) attending court on the return date to potentially release things removed from the respondent’s premises.

The independent solicitor – computers, no ICE

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”.¹¹ >>

>>

It is submitted that this discretionary power should only apply when an ICE was not appointed, as computers were not envisaged as part of the search order.¹²

The Pro-forma Search Order¹³ 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.¹⁴

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.

Independent computer expert

The ICE is an essential member of the search party when computers are anticipated as part of a search order. However, the Supreme Court Practice Direction currently provides no guidance or clarification as to the qualifications and experience required for an individual to be appointed as an ICE.

Notwithstanding this, 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.¹⁵ This is essential to developing strategies to assist legal professionals identify,¹⁶ 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.¹⁷

In particular, the role of the ICE may include:

- (a) searching the respondent’s computers for listed things in the form of ESI¹⁸
- (b) making a copy of one or more computer hard drives¹⁹
- (c) ensuring a chain of custody is maintained for each computer hard drive and copies thereof,²⁰ and
- (d) producing a report as to the performance of their preliminary findings, generally includ-

ing their search regime, a directory and file listing of ESI contained on the forensic images of the hard drives.²¹

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 in terms of the relevant order.

Reasonable endeavours, minimal disruption and hard drives

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 image²² of the one or more physical hard drives within the computer (physical forensic imaging).²³ Creating a forensic image of even an ‘average sized’ computer hard drive can be time intensive. As mentioned above, this clearly has the potential to cause disruption to the respondent.

Emerging computer forensics techniques, variously referred to as ‘live forensics’, facilitate forensic imaging whilst the computer is still running and in operation,²⁴ resulting in little or no downtime to the respondent’s com-

Notes

- 1 Seamus E. Byrne LL.B., CISSP, CCE, EnCE – Lawyer and director, forensic technology, Vincents Chartered Accountants (www.seamusbyrne.com).
- 2 Geoffrey Lambert LL.B., GCLP.
- 3 *Uniform Civil Procedure Rules 1999* (Qld) R 261. See also *Federal Court Rules* O 25B.
- 4 M. Holler, ‘Anton Piller orders in Australia: lessons from other jurisdictions and suggested refinements for Australia’ (2005) 32(9) *Brief* 10-17.
- 5 *Anton Piller KG v Manufacturing Processes Ltd* [1976] Ch 55.
- 6 Supreme Court of Queensland, Practice Direction 2/2007 (May 8, 2007).
- 7 Federal Court of Australia, Practice Note 24 (May 5, 2006).
- As at time of writing, see other Australian jurisdictions which have introduced the harmonised practice guidelines: Supreme Court of New South Wales, Practice Note SC Gen 13 (June 14, 2006).
- Supreme Court of Tasmania, Practice Direction 4/2006 (July 19, 2006).
- Supreme Court of South Australia, Practice Direction 4.3 (September 4, 2006).
- Supreme Court of Victoria, Practice Note 2/2006 (September 1, 2006).
- Supreme Court of the Northern Territory, Practice Direction 6/2006 (November 27, 2006).
- Supreme Court of Western Australia, Practice Direction 6/2007 (May 2, 2007).
- 8 This was also recognised at common law, see: *Microsoft Corporation v Goodview Electronics Pty Ltd* [1999] FCA 754, [30-31] (per Branson J).
- 9 Supreme Court of Queensland, Practice Direction 2/2007 (May 8, 2007), [7].
- 10 Pro-forma Search Order, [13] (Appendix to Supreme Court of Queensland, Practice Direction 2/2007 (May 8, 2007)).
- 11 Supreme Court of Queensland, Practice Direction 2/2007 (May 8, 2007), [7(g)].
- 12 Notwithstanding, it would be considered almost foolish. Given the commercial circumstances generally associated with the granting of such orders, it is often the case that a wide range of ESI will be available within and upon a myriad of electronic repositories and media.
- 13 Pro-forma Search Order, Schedule B.
- 14 *GT Corporation Pty Ltd v Amare Safety Pty Ltd* [2007] VSC 123, *Oke v Commissioner of the Australian Federal Police* [2007] FCA 27, *Prescience Communications Ltd v Commissioner of Taxation Office* [2006] FCA 1561, *JMA Accounting Pty Ltd v Commissioner of Taxation* [2004] FCA 274.
- 15 Cath Everett, ‘Cred or Crud’ (2005) 2(4) *Digital Investigation*, 237-238. See also: John Barbara, ‘Digital evidence accreditation in the corporate and business environment’ (2005) 2(2) *Digital Investigation*, 137-146. Nigel Jones, ‘Training and accreditation – who are the experts?’ (2004) 1(3) *Digital Investigation*, 189-194.
- 16 Supreme Court of Queensland, Practice Direction 2/2007 (May 8, 2007), [3].
- 17 Eoghan Casey, ‘Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet’, (2nd ed., 2004). Standards Australia, ‘Guidelines for the management of IT evidence’ (HB 171-2003) (2003).
- 18 Supreme Court of Queensland, Practice Direction 2/2007 (May 8, 2007), [6], Pro-forma Search Order, [18(b)].
- 19 Pro-forma Search Order, [18(c-d)].
- 20 Pro-forma Search Order, [18(e)].
- 21 Pro-forma Search Order, [18(e)].
- 22 Also referred to as a ‘bit-stream copy’.
- 23 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 practitioner.
- 24 Some business and mission-critical computers cannot be turned off at all without significant risk of damage or data loss.
- 25 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.
- 26 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 their expertise.
- 27 Pro-forma Search Order, [9].
- 28 Pro-forma Search Order, [14].
- 29 In Queensland, evidence destruction is arguably addressed by *Criminal Code Act 1899* (Qld) s125. See: *R v Ensbeay* [2004] QCA 335. 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*.
- 30 Where a respondent is not a corporation, they may also gather things which they believe may tend to incriminate them or make them liable to a civil penalty using the same process per paragraph 10(c) of the Pro-forma Search Order. Under paragraphs 21-22 of the Pro-forma Search Order, additional supporting affidavits may be required to be served on the applicant.
- 31 Pro-forma Search Order, [11].
- 32 Pro forma Search Order, [20].
- 33 Supreme Court of Queensland, Practice Direction 2/2007 (May 8, 2007), [16(c)].
- 34 Pro-forma Search Order, [19(b)]. Also, where a respondent is not a corporation, they may also object to material on a computer which they believe may tend to incriminate them or make them liable to a civil penalty: paragraph 19(a) of the Pro-forma Search Order. Under paragraphs 21-22 of the Pro-forma Search Order, additional supporting affidavits may be required to be served on the applicant.
- 35 Pro-forma Search Order, [19(c)].
- 36 Pro-forma Search Order, [19(c)(i)].
- 37 Pro forma Search Order, [20].
- 38 Pro-forma Search Order, [19(c)(ii)].
- 39 See [13].
- 40 *Aristocrat Technologies Australia Pty Ltd v Global Gaming Supplies Pty Ltd* [2006] FCA 1707, [21] (per Jacobson J).

The revised practice guidelines have arguably resulted in increased and timely judicial consideration of significant issues related to ESI.



puter (and business operations which rely upon such computers). 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, the scope of what is forensically copied could be limited to all Microsoft Word documents within a certain user's folders or directory.²⁵

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.²⁶

Computers & the respondent

Subject to the restrictions on entry, search and removal, the respondent must:

(a) disclose the location of "all computers, computer disks and electronic information storage devices . . ."

(b) provide all necessary passwords to access and operate computers

(c) permit an ICE to search any computer and make a copy of any computer hard drive, and

(d) permit an ICE or the independent solicitor to remove any computer or computer hard drive.²⁷

From the time prior to admitting entry to the search party until the return date, the respondent also must "not disturb or remove any listed things".²⁸ 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.²⁹

Dealing with claims of privilege

The Supreme Court Practice Direction sets out the following procedures for dealing with privilege claims as part of a search order:

Hard-copy documents

(a) 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 for sealed envelope or container.³⁰ Anything provided via this method is not to be inspected by anyone until the return date.³¹

(b) Prior to the return date, the respondent shall be entitled, in the presence of the inde-

pendent 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.³²

(c) On the return date, privilege claims are to be considered.³³

Computers and electronically stored information (ESI)

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

(a) The respondent is entitled to object to the conduct of the ICE on the ground that the computer contains material that is otherwise privileged.³⁴

(b) Upon making the objection, the conduct of the ICE becomes inoperative to the extent of the objection. For example, the ICE may be restricted from searching and creating a forensic image of one or more computers.³⁵

(c) 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.³⁶

(d) 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.³⁷

(e) On the return date, privilege claims are to be adjudicated.³⁸

The practice guidelines in practice

Recent case law and decisions involving the Federal Court Practice Note³⁹ have highlighted the myriad of issues faced by lawyers when addressing strategies to search and manage large volumes of ESI with respect to privileged and confidential information.⁴⁰ The revised practice guidelines have arguably resulted in increased and timely judicial consideration of significant issues related to ESI. Given the continued ubiquity of ESI, it is submitted that:

(a) Authoritative and accepted standards, guidelines, accreditations or qualifications regarding ICEs 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.

(b) 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.

(c) 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. ■