



[Home](#)

[About Us](#)

[Current Issue](#)

[Law Firm News](#)

[Dealmakers](#)

[Get A Life!](#)

[Careers centre - NEW!!](#)

[2008 Best Dressed Lawyers - NEW!!](#)

[Law Awards](#)

[Expert Witness Directory](#)

[Professional Development](#)

[Specialist Reports](#)

[Archives](#)

[Subscribe](#)

[Advertise](#)

[Contact Us](#)

[Useful Links](#)

How to catch an electronic thief

Campbell McKenzie and Sarah Armstrong discuss the benefits of using forensic computing techniques during an Anton Piller order

Anton Piller orders are often described as the 'nuclear weapon' of a civil litigator's armoury. They are a form of ex parte urgent injunctive relief which allows for the search and seizure of relevant documents to a proceeding in circumstances where "if the defendant was forewarned, there would be a serious risk of destruction".

The Anton Piller order arose out of a 1976 decision of the English Court, before the age of computers and technology (Anton Piller KG v Manufacturing Processes Ltd [1976] 1 All ER 779).

Fast-forwarding 30 years, it is now common to locate a computer system in every home and business, each typically containing over 50,000 files, many of which may contain evidence of offending. In addition, relevant files may also be stored on hand-held devices, USB keys, and other backup media such as disk or tape.

How to manage the electronic evidence

With the modern world's reliance on electronic devices, it has become common practice to obtain electronic data for the purpose of legal proceedings. Due to demand, forensic computing experts are now employed in both the public and private sectors to assist investigators in the searching, seizing, and reviewing of electronic data. The experts are relied on to maintain a chain of custody, to ensure evidential integrity, and to recreate a series of events involving electronic devices.

The services of forensic computing experts are increasingly being engaged to investigate and assist in cases involving fraud, breach of confidence, breach of copyright, employment issues, and electronic discovery requests. A suspecting employer may have an ex-staff member's computer analysed to reveal files that have been copied and incriminating communications. While informative, the evidence is limited to the historical activities of the employee. An Anton Piller order, however, has the added benefit of allowing access to the defendant's home or new work computer. This may then prove that the plaintiff's confidential information is in the possession of the defendant, and, more importantly, being amended and printed for the purposes of competitive business.

Civil search and seizure orders

A number of alternatives are available when considering civil search and seizure orders (such as Anton Piller orders, preservation of property orders (High Court Rule 331), orders for inspection (High Court Rule 332), and injunctions under the Employment Relations Act 2000).

The Anton Piller order allows the court to grant an order allowing a party's solicitor, accompanied by an independent solicitor, to search premises and seize evidence without prior warning. It requires the owner or occupier to provide their

consent for the search, or otherwise apply for the order to be discharged.

As an Anton Piller is on an ex parte basis and is invasive, they are only issued in exceptional circumstances and in accordance with the three-step test set out by Lord Justice Ormrod in the Anton Piller decision:

- There is an extremely strong prima facie case against the respondent;
- The damage, potential or actual, must be very serious for the applicant; and
- There must be clear evidence that the respondents have in their possession incriminating materials and that there is a real possibility that they may destroy such material before an application or notice can be made.

The practicalities of obtaining an Anton Piller order

It is important to do the following before seeking an Anton Piller order:

- Identify nature of and likely location of relevant materials.
- Obtain evidence that the materials are likely to be in the party's possession. If the relevant data is stored electronically, this is best done through a forensic IT expert.
- Appoint an experienced IT expert and supervising lawyer to assist with the execution of the order. You will often need to identify these individuals to the Court so it is important to check their availability in advance. If the order is to be executed at a residential address, it is good practice to ensure that one of the people authorised to be present for the search is a female.

Scope of the order

Time must be taken in drafting the order to ensure that it is wide enough to enable a search that will provide you with the relevant information. It is often invaluable to liaise closely with your IT expert when preparing the draft order to ensure that it adequately covers the forensic work they will need to perform on the defendant's computers. For example, the order should require the defendants to provide passwords and, where relevant, email account numbers. It may also seek authority for a representative from the plaintiff to be present if specialist knowledge is required to identify the plaintiff's property.

The plaintiff's solicitors are under a duty not to seek an order in unnecessarily wide terms. The filed papers must attach a draft order. The Court may well require you to justify the scope of the orders sought, and it is not uncommon for amendments to be made after a short hearing with a judge and prior to the order being granted. As a consequence, there is very little case law to provide explicit guidance on the terms on which the order should be made. The balancing exercise is to frame the orders wide enough to carry out the purpose of preserving evidence, while at the same time minimising the interference to the defendants (and their families if the order is to be executed at a residential address).

If it is later discovered the motive behind the order was to destroy the defendant's business rather than to preserve evidence, the Court may order aggravated damages or the immediate discharge of the order. One way to avoid an inference that the motive was to destroy the defendant's business is to take a forensic copy of the computer system and photocopy the hard copy documents so that the defendant's business operations do not need to be put on hold to carry out the order.

Execution requires careful organisation and orchestration. If there are multiple orders, the execution must be carried out at the same time to avoid notice being given to the occupiers of different premises. The order should be carried out at a time when there will be someone present at the premises to let you in. If entry is refused, be prepared to seek contempt orders. The main area of abuse has taken place in the execution of orders. The terms of the order must be carefully adhered to and the principle of minimum interference (ie no more should be done than is necessary to

achieve the purpose of the order) should be followed.

The search will begin once the defendant has accepted the order. The defendant will be given a reasonable time to obtain legal advice before the search commences. The legal counsel of the defendant may choose to appear to assist in interpreting the order and monitoring the search.

The search process must be well documented and enable identification of the location from which an item was removed. It is useful to bring a receipt book with carbon copies for the lawyer, the recipient, and the independent solicitor, so that each independent item can be identified and receipted. In respect of electronic data, the normal approach is to obtain a forensic copy of the entire data to enable for the search and identification of the relevant data that falls within the order. The independent lawyer must later report to the Court on how the search was conducted and what was found.

Electronic considerations for the Anton Piller order

Perhaps the quote "expect the best, plan for the worst, and prepare to be surprised" sums up the typical electronic search and seizure exercise. Variations in hardware, software, and the defendant's reaction will all impact on the execution of the order. In preparing for a range of eventualities, consider the following:

- Seek orders that do not state a requirement to locate electronic evidence on site. It is easy to underestimate the search process, especially for deleted or compressed data.
- Even with high-speed copying systems, a hard drive may take over three hours to copy, and it is preferable for all parties involved to start this process as soon as possible.
- The definition of 'confidential information' must be specific and not broad to the point of being ambiguous.
- Look to seize any data device that contains the plaintiff's confidential information to avoid the potential of further usage.
- Seek to obtain orders that state the forensic computing expert can retain exhibits and forensic copies. This will minimise any unnecessary delays in having to access the data from an independent lawyer.
- A suitable resolution such as the wiping of data can be agreed to shortly after the execution of the orders.

It is always preferable to take a full forensic copy of an electronic device, which will include any potentially deleted data. In the event a defendant refuses a full forensic copy, a partial copy may be considered, which will limit the copying to non-deleted data, such as active Microsoft Word documents.

The collection of electronic evidence using forensic methodologies will provide a platform from which to review the data for relevant information. The success of the examination will depend on both the skills of the expert, and the suite of forensic software tools used. In order to locate some of the relevant documents, advanced data and password recovery techniques may be relied upon.

In order to prove that confidential business information has been stolen, the expert may conduct a comparison of each party's files to determine exact matches. Further, evidence of accessing, modifying, and publishing these documents may be located both in the metadata of the documents and through system files such as 'link' files.

With the potential of locating a vast number of relevant documents, and in preparation for legal proceedings, the latest electronic discovery tools can be used to index all data (including Adobe PDF files), and then exported directly into Summation and Ringtail with metadata attached. Once in this format, documents can be classified as either relevant, irrelevant, or privileged.

Perhaps the most valuable skill the forensic computing expert possesses is the ability to irretrievably wipe the plaintiff's confidential information from the defendant's hard drive, which, after all, is the purpose of the Anton Piller.

Campbell McKenzie is an associate director in the Investigations and Forensic Services team at PricewaterhouseCoopers. Sarah Armstrong is a partner in the General Litigation team at Russell McVeagh.

NZLawyer, 16 May 2008