



Roger Partridge Partner

Search warrants: key new court ruling

Investigators given new warnings for the electronic age

Search warrants by their very nature will always be fraught with contention - but a recent court ruling places new pegs in the ground.

At the heart of the findings are measures to safeguard against "fishing expeditions", particularly in the new electronic environment, and the need to develop a practical approach to protecting documents covered by legal professional privilege.

The findings of the Court of Appeal in *Director of the Serious Fraud Office v A Firm of Solicitors* go some way to resolving these difficult issues, but stop short of prescribing a procedure to be applied in practice. For this reason, it is likely that disputes will continue to arise in relation to search warrants.

Search warrants, computer records and legal professional privilege

The Courts have consistently upheld the fundamental importance of the right to seek legal advice in confidence and, where necessary, resist disclosure of such advice by asserting legal professional privilege. Central to this right is that, in the absence of express statutory authorisation, the Courts may not issue search warrants that purport

to permit the seizure of privileged material.

This presents an acute problem for investigators who wish to seize material stored in computers. Computers are likely to contain thousands (in some cases millions) of documents, many of which will be privileged and most of which will be irrelevant. Investigators do not generally have any right to seize privileged or irrelevant material. As a matter of principle, it should make no difference if the documents are in hard copy or stored in a computer.

Equally however, it is impractical for investigators to review each file on each computer at the time the warrant is executed. This is especially true if it is necessary to forensically examine the computer to retrieve deleted material.

The usual procedures for executing search warrants do not offer a satisfactory solution to this difficult situation.

A series of recent cases left the law in this area uncertain, and it has largely been left to the parties in each case to negotiate a pragmatic solution. The Court of Appeal was faced with this kind of situation in *Director of the Serious Fraud Office v A Firm of Solicitors*.

The case: Director of the Serious Fraud Office v A Firm of Solicitors

The case concerned a warrant obtained by the Serious Fraud Office (SFO) to search the premises of a law firm, which the SFO suspected had engaged in fraud.

The SFO applied for a search warrant with an accompanying affidavit setting out the alleged involvement of two partners in the firm - but it failed to mention that the partners had been interviewed by the SFO, and that they had accepted that they held relevant documentation and had offered to co-operate with the investigation.

A District Court Judge issued the warrant, which was executed the next day. The SFO and an independent computer expert seized paper files and six computers, including a server, which were taken away and cloned. It undertook that the clones would be accessible by a password known only to the independent computer expert, and that the material would be sealed pending the resolution of privilege issues. This is the procedure commonly adopted by regulators in this kind of situation.

The firm applied for judicial review of the decision to issue the warrant. In the High Court, Heath J held that the warrant was invalid. The issues on appeal included:

- Whether the warrant was invalidated by the failure to disclose relevant information to the Judge;
- Whether the warrant stated with sufficient specificity the documents sought; and
- Whether the warrant could validly allow the removal of computers containing privileged material.

Parties applying for a search warrant must disclose all facts that could reasonably be regarded as relevant.

The Court emphasised this point of disclosure. The fact that, with the benefit of hindsight, a particular matter may not be so fundamental as to justify invalidating a warrant does not necessarily mean that the information could not reasonably be regarded as relevant.

When it applied for the warrant, the SFO should have disclosed that the partners had already accepted that they had relevant documents, and had agreed to co-operate with the investigation. As this information was not revealed, proper disclosure had not been made, and as a result the warrant was invalid.

Search warrants must specifically state the documents sought.

The Serious Fraud Office Act does not expressly require that search warrants specify the documents that are being sought under the warrant. Relying on this, and the general wording in the prescribed form for the warrant, the SFO sought and obtained a general warrant that did not identify the documents that were the target of the search.

The Court of Appeal held that the warrant was invalid for this lack of specificity. In the absence of an express statutory exception, all search warrants must be "as specific as the circumstances allow". The Court rejected the argument that the absence of an express requirement in the Act for specificity justified the use of general warrants.

In particular, the warrant should not have purported to authorise the removal of whole computers. While it may have been appropriate for the warrant to identify these as items to be searched for relevant evidence, it could not be said that they were themselves items of relevance.

The Court further held that, on the facts of this case, there was no reason for the SFO



Tim Fitzgerald Solicitor

not to be specific about the documents sought. The SFO had already obtained information about the fraud which allowed it to exclude the vast bulk of the firm's documents and electronic data from the ambit of the search.

Search warrants must adequately protect the rights of those being searched to assert legal privilege.

Although it had already found that the warrant was invalid, the Court went on to consider whether it was possible for an appropriately specific warrant to authorise the removal and cloning of a hard drive containing privileged and/or irrelevant material, in addition to the information legitimately sought.

The Court acknowledged that hard drives which are known to contain relevant non-privileged material may need to be cloned to give effect to the warrant. It held that they may be removed only if:

- There are reasonable grounds to believe that there is relevant data stored on the hard drive;
- This evidence cannot be extracted from the hard drive without the use of forensic investigative techniques;
- It is not practicable to carry out those extraction measures on-site without the risk of destruction or unsuccessful extraction of the evidence; and
- There is no practicable alternative to removing the hard drive itself for the purposes of undertaking the extraction measures off-site.

The Court likened a computer to a book or very long document containing a combination of relevant, irrelevant and privileged material. The fact that the book contained irrelevant or privileged material should not prevent the investigators from removing it – they would not be expected to read the book and tear out the relevant and non-privileged pages on

site. What would be required in this situation is a clear procedure to protect privileged material without frustrating the ability of the investigator to search for relevant material.

Where these criteria are met, a search warrant may be issued which permits the removal and cloning of the hard drive, provided that:

- The warrant is issued on terms that preserve the right of the investigated party not to disclose any privileged communication;
- The warrant contains conditions ensuring that irrelevant material is not accessed, except where unavoidable for the purposes of assessing its relevance, and that this material is deleted or returned after extraction of the relevant material; and
- The issuing judge is satisfied, on the basis of clear evidence, that there is no practical alternative to cloning.

The Court observed that “extensive conditions” were needed to protect privileged material and that “it may well be appropriate” for an independent lawyer to be present at the search to be able to report back to the issuing judge on the conduct of the search and to ensure that the safeguards set out in the warrant are followed.

The onus to ensure that these conditions are in place was placed firmly on the party seeking the warrant. The need to instruct senior counsel in some cases was explicitly referred to.

Importantly, the Court also said, except in cases of utmost urgency, the Court should be given (and should insist upon) enough time to read all the papers carefully and question counsel about the legal issues involved.

To receive your updates faster, please subscribe to our electronic newsletter service on: info@bellgully.com

To view all our publications or update your details please visit our website: www.bellgully.com

For further information, please contact your usual Bell Gully advisor or:

AUCKLAND

Roger Partridge

roger.partridge@bellgully.com
64 9 916 8922

Tim Fitzgerald

tim.fitzgerald@bellgully.com
64 9 916 8859

Disclaimer: This publication is necessarily brief and general in nature. You should seek professional advice before taking any further action in relation to the matters dealt with in this publication.
All rights reserved © Bell Gully 2005.

The reasoning was specific to the Serious Fraud Office Act and the position of other statutes was not considered. However, there is little reason to believe that a different approach would be taken elsewhere.

Implications of the decision

There are many welcome aspects of the Court's decision. For one, it affirms that it is not enough merely to identify in broad terms the suspicions on which the warrant was sought. Regulators must identify specifically the documents sought under the warrant.

Even more importantly, the Court emphasised the primacy of legal professional privilege. Regulators may not apply for, and the Court may not issue, warrants that authorise the seizure of privileged material. This includes material on computers and other electronic media that may also contain relevant and non-privileged documents.

What the Court did not do is explicitly set out a procedure for protecting privileged material. As a result, it is likely that disputes will continue to arise relating to the adequacy of procedures set out in search warrants.

Encouragingly, however, the Court has set out a framework for the resolution of these disputes that emphasises the obligations of the party obtaining the warrant to make full, balanced and considered disclosure to the issuing judge and to provide a fair procedure to protect privileged information.

It also highlights the need for judges issuing search warrants to pay close attention to the procedures they contain to ensure that these protections are in place.

Hopefully investigators will heed these warnings and this will lead to the

development of standard procedures that both enable effective searches and provide proper protection for the privileged material of those under investigation.

AUCKLAND
Vero Centre
48 Shortland Street
PO Box 4199, Auckland
New Zealand, DX CP20509
Telephone 64 9 916 8800
Facsimile 64 9 916 8801

WELLINGTON
HP Tower
171 Featherston Street
PO Box 1291, Wellington
New Zealand, DX SX11164
Telephone 64 4 473 7777
Facsimile 64 4 473 3845

www.bellgully.com

Bell Gully