

## The risks of self-help remedies in cyber crime investigations

INFORMATION TECHNOLOGY HAS SOLVED MANY long-forgotten problems. It has also, however, thrown up its own issues, often on an unprecedented scale. One of those issues is cyber crime.

When investigating cyber crime, the inclination can be to use all the tools at one's disposal and to do all that is necessary to acquire information to establish what happened, who is responsible and to recover what has been stolen.

However, the potential risks involved in adopting such an approach cannot be over emphasised, and it is crucial that any investigation is conducted lawfully.

Often, the steps taken at the outset of an investigation can damage, rather than advance, the ability to recover what has been stolen. Those undertaking investigations should have the requisite technical, organisational and legal knowledge, and, where this is not the case, it is essential that appropriate external assistance is sought.

### GOING IT ALONE

The recent case of *L v L and another* provides a salutary lesson in this area. A Swedish woman, in the throes of a divorce, employed a computer expert to remove and copy a laptop belonging to her husband. Two copies of the hard drive were taken before the laptop was returned to the family home. The wife took this precaution as she feared the husband intended to destroy evidence that would assist her case.

The wife claimed that her husband had thrown out a number of documents that had been kept in his office at the family home. In correspondence produced to the Court, the wife's solicitors stated that they had advised her that it would be a sensible precaution to obtain a copy of the hard drive as this was virtually the only repository of documentary information left in the home. They said that they gave the advice when told that the husband had shredded some documents, and they were aware that he had recently changed the password.

The husband claimed that he had acted openly and innocently, and pointed to the fact that there were no proceedings in existence or in contemplation at that time save for the Swedish proceedings (which his wife had previously begun) for which, he said, no documents were required.

On 9 November 2006 the wife commenced her family law proceedings in England. On 16 November 2006 the husband commenced his own proceedings against both the wife and her solicitors seeking the delivery up of all copies of the hard drive. Injunctive relief was also sought to restrain the defendants from communicating or disclosing the contents of the hard drive.

The husband claimed that the contents of the hard drive contained documents that fell within the categories of legal professional privilege, information that was not privileged and was possibly relevant to the wife's proceedings, and personal and business information that was not relevant to the wife's proceedings.

The husband pleaded that the taking and copying of his hard drive constituted a breach of his rights in privacy, confidentiality and legal professional privilege, as well as being in contravention of the Data Protection Act 1998 (the 1998 Act). It was additionally argued at the hearing that the wife and her solicitors were in breach of s55 of the 1998 Act (obtaining or procuring personal data in breach of the Act) and s1 of the Computer Misuse Act 1990 (obtaining unlawful access to a computer), both of which were criminal offences.

In their defence, the wife and her solicitors claimed that the contents of the hard drive had been copied for the purpose of preserving evidence of the claimant's financial position, which may have otherwise been destroyed by him. This, it was alleged, ensured the proper administration of justice in the wife's proceedings. They responded to the claims made under 1998 Act by relying on ss35 and 36, which relate to disclosures required by law or made in connection with legal proceedings, and exemptions for data processed by an individual for the purpose of that individual's personal, family or household affairs respectively.

The Court decided that there had been no reason why the wife could not have made an application for a search or seizure order, although they believed she would have been hard pushed to have established sufficient evidence for such an order to be granted.

The Court also expressed considerable concern that parties to litigation should conduct searches that

**'The fact that there may be good grounds for conducting an investigation does not mean the end justifies the means.'**

Anthony Riem, partner, PCB Litigation LLP  
E-mail: [ajr@pcbllitigation.com](mailto:ajr@pcbllitigation.com)



lack any of the safeguards built into search orders issued by the courts. In this case, the wife was seeking to retain a position that she occupied by self-help, when, on the evidence available, she could not have got herself into that position by an application to the Court.

The Court then considered the implication of evidence having been unlawfully obtained in a civil matter. The fact that the wife might, in the circumstances, be permitted to obtain some advantage from evidence obtained unlawfully was one reason for the Court to conclude that the balance of justice favoured the interim delivery up of the copies of the hard drive to the husband's solicitors.

The decision in this case serves as a warning both to solicitors and victims of cyber crime as to the potential risks that may be involved when using self-help remedies.

#### PRETEXTING

Companies also need to take care when employing external agencies to undertake investigations. As Hewlett Packard's former chairwoman, Patricia Dunn, found, employing those who use surreptitious methods in their investigations can cost you your job.

Dunn ordered an investigation into media leaks about corporate strategy, HP's interest in buying another company and discussions concerning its next CEO. Unfortunately for her, the external agency employed to carry out the investigation used a method called 'pretexting'. This involved posing as someone else in order to acquire the telephone records of reporters and board members suspected of involvement in press leaks.

Although it was clearly essential for an investigation to be carried out to identify and stop the source of the leaks, and Dunn made it clear that she had no knowledge that unlawful means were apparently being used, this did not prevent her from having to appear before a congressional subcommittee and from criminal charges being made against her, which she denied, and which were subsequently dropped.

The issue of pretexting was also addressed in *Dubai Aluminium Co Ltd v Al Alawi and others*, in which PCB Litigation LLP successfully represented the defendant. This case required the Court to decide whether the claimants were entitled to claim legal professional privilege in relation to documents allegedly obtained by agents through pretexting.

The defendant sought discovery of the documents, which related to the investigation of him undertaken by the agents. The claimants accepted that such documents were relevant and discoverable, but claimed that legal professional privilege attached to them. The Court found that, although there was a very strong public interest in legal professional privilege, there was also public interest in combatting fraud and in protecting the victims, or potential victims, of such a crime. It therefore ordered the claimant to provide disclosure of legally privileged material that would otherwise have been protected from disclosure.

These cases provide a vivid illustration of the pitfalls that can be encountered when carrying out an investigation, and the reason why obtaining professional advice at the outset is so important.

#### MISUSE OF PERSONAL INFORMATION

It is not just falling foul of the law in the actions taken to obtain information which must be considered. The type of information obtained is also a concern.

These days, personal information is more highly protected than ever before. The 1998 Act provides for criminal sanctions to be taken against those who misuse personal information. It is an offence to 'obtain or disclose personal data or information contained in personal data or procure the disclosure to another person of the information contained in personal data' (s56 of the 1988 Act). This means that it is not only those who are employed to undertake investigations who may be held criminally liable, but also those who employ them.

The methods used in the acquisition of personal data are the subject of statutory regulation and can incur criminal sanctions, including imprisonment, if the law is breached.

This area comes under the Regulation of Investigatory Powers Act 2000 (the 2000 Act), which has replaced the Interception of Communications Act 1985 to take account of advances in technology and in particular, the use of e-mail and the internet. Under the 2000 Act, it is an offence to intentionally intercept any communication in the course of its transmission by means of public postal service or public telecommunications system.

However, under Regulations that have come into force as a result of powers granted to the Secretary of State by the 2000 Act, businesses may intercept e-mails in specified circumstances without the consent of the sender or the recipient. >

**COMMENT**

As we have seen, there are many areas to consider when undertaking a self-help investigation in order to avoid doing more damage than good. Theft of information, particularly cyber information, is a fast-growing and worldwide phenomenon. Employees often view information as marketable and a means of gaining a commercial and legal advantage, and employers will often require investigations to take place.

For example, on 2 March 2007, *The Times* reported that the Ikos group of companies has issued proceedings against two former workers, twin brothers Lucian and Julian Gover, for the return of confidential computer files holding client details. The brothers readily admit taking documents and computer records, but one is quoted as saying: 'After a 13-year relationship, Ikos wanted us to leave the company for reasons unknown. All commercial decisions have an

economic consequence. In this case it's the requirement to make a fair and equitable payment to us upon our departure from the firm. That's what we're looking for.'

Although it will be interesting to see how the court will deal with the arguments that the parties put forward to substantiate their positions, it is clear that a party that relies on self-help remedies does so at its own risk. The fact that there may be very good grounds for conducting an investigation does not mean that the end justifies the means. If a party contemplates taking an unusual step in an investigation, it is usually better to obtain the court's sanction beforehand.

*By Anthony Riem, partner, international fraud and commercial litigation, PCB Litigation.*

*E-mail: [ajr@pcbllitigation.com](mailto:ajr@pcbllitigation.com).*

*Tel: +44 (0)20 7831 2691.*

*[www.pcbllitigation.com](http://www.pcbllitigation.com).*

---

*L v L and another [2007] EWHC 140 QB*

---

*Dubai Aluminium Co Ltd v Al Alawi and others [1999] 1 All ER 703*