Accessing the Other Side's Computers?
Imaging and Inspection Orders

Peter Linstead, Outer Temple Chambers

Applications for orders permitting a search of a defendant's computers and electronic devices are routinely sought in cases involving employee competition and claims based on the misappropriation of IP. This is commonly at the outset of proceedings, in tandem with an interim injunction application. The High Court has been receptive to these applications in the last few years, to varying degrees. This article considers the reasons for, and the limits of, these applications, including a recent pronouncement on the relevant principles by the Court of Appeal.

Peter Linstead, the author of this article, has recently published a book on employee competition: "*Restraining Competition by Employees: A Practical Guide to Restrictive Covenants, Injunctions and Other Remedies*" in which computer imaging and inspection orders are considered in more detail.

It is at first sight surprising that one party should be allowed access to another's stored information. In a normal civil claim, each party makes its own disclosure (including e-disclosure) as a step in proceedings, often followed by specific disclosure applications.

What are the different types of order?

The starting point is that there are three distinct types of order which might be granted.

The first is as a form of search order made without notice before proceedings have commenced under CPR rule 25.1(1)(h) (formerly known as an *Anton Piller* order). The courts have recognised that a search of someone's electronic life can be just as intrusive as searching their premises without warning and is likely to engage the right to privacy under Article 8 of the European Convention on Human Rights. There is a high threshold for justifying this: the applicant must show that "there is grave danger of property being smuggled away or of vital evidence being destroyed" (per Lord Denning in *Anton Piller KG v Manufacturing Processes Ltd* [1976] Ch 55).

Nevertheless, an application might succeed where it is shown that putative defendants are likely to erase information and wipe devices, to cover their tracks. There are various onerous conditions, including the duty of full and frank disclosure. Just as a Supervising Solicitor would be appointed to serve the order and supervise the search in the case of a physical search, a supervising independent IT expert will be generally required.

The second is an order for computer imaging and inspection, sought on notice but at an early stage. It is often ordered at the same 'on notice' interim relief hearing at which an injunction is sought. Such an order would be made under CPR rule 25.1(1)(c)(i) which applies to the detention, preservation and inspection of property.

A third category of order is the 'delivery up order', which could also be made under CPR rule 25.1(c)(i), to include electronic documents or information. However, where the delivery up of electronic documents is sought without notice, this can be hard to distinguish from a search order and is known as a 'doorstep delivery up order' – a reference to the delivery up to a solicitor on the defendant's doorstep. CPR 25A PD 8.2 provides that where a delivery up order is made, consideration is given by the court to whether, for the protection of parties, similar provisions should be put in place to those specified for a search order. This could include a Supervising Solicitor. An 'on notice' application is much less intrusive, and might require a party to deliver electronic documents or information to the claimant's solicitor at a specified time. On the face of it, delivery up orders do not require one party to access another's systems, but applications are sometimes made to allow access to an independent IT expert to supervise the process.

What is the justification for such an invasive order?

An authoritative list of relevant factors was given by Akenhead J in *McLennan Architects Ltd v Jones* [2014] EWHC 2604 (TCC). These are set out below, but the touchstone is that the order must be necessary and proportionate:

(a) The scope of the investigation must be proportionate.
(b) The investigation must be limited to what is reasonably necessary.
(c) Regard should be had for the likely contents of the device sought so that any search should exclude possible disclosure of privileged documents or documents irrelevant to the case.
(d) Regard should be had to the human rights of those whose information is on the device and the relevance of any such information to the case.
(e) Access to a complete hard drive would rarely be granted unless dedicated to a particular contract or project.
(f) The court should require a confidentiality undertaking from any expert or other person given access to the relevant electronic devices.

There is an important distinction to be made between disk imaging and an order which permits inspection of the contents of a defendant's computer system.

The importance of this distinction was recently emphasised by the Court of Appeal (in the context of search orders) in *TBD (Owen Holland) Ltd v Simons* [2020] EWCA Civ 1182. Arnold LJ stated that the purpose of a search order is to preserve evidence and/or property in order to prevent the defendant from altering, destroying or hiding it if given notice. The facts that justify a search order being made might also in appropriate cases justify without notice orders for the disclosure and inspection of documents and/or the provision of information pursuant to either CPR Part 18 or the court's inherent jurisdiction. Nevertheless, the two types of orders "*are distinct, require separate justification, have different effects and must not be conflated*". Both types of order must contain proper safeguards, which will be different for each type.

It is worth asking why such orders are made in employment and intellectual property cases and why standard disclosure is not enough.

The order will invariably be sought at the same time as an injunction. By definition, these are cases where damages are not an adequate remedy and the court will have to be satisfied that in order to stop unlawful activity, the claimant needs to be able to obtain knowledge of the defendant's activities now, which the defendant cannot be trusted to provide. Nevertheless, the orders are still derived from the jurisdiction of the court to order disclosure.

How far can a claimant go?

The need to preserve evidence will be met by an order allowing for imaging a defendant's hard drive. A compelling argument will be needed to justify searches being carried out by the claimant. It is particularly unlikely that an order on a 'without notice' application will go any further than an imaging order. In *TBD (Owen Holland) Ltd v Simons*, Arnold LJ stated:

"…the basic safeguard required in imaging orders is that, save in exceptional cases, the images should be kept in the safekeeping of the forensic computer expert, and not searched or inspected by anyone, until the return date. If there is to be any departure from this, it will require a very high degree of justification, and must be specifically and explicitly approved by the court."

When the application is made to inspect the imaged systems, the court will have to deal with the significant risk that the search might cause the claimant to view the defendant's own confidential material as well as privileged material. Crucially, Arnold LJ stated that on the return date, there is a presumption that it will be for the defendant to give disclosure of such documents in the normal way. He said that whilst that may be departed from where there is sufficient justification:

"…there should be no unilateral searching of the images by or on behalf of the claimant: the methodology of the search must be either agreed between the parties or approved by the court." (at [193])

Sometimes, in addition to an order allowing a search, claimants seek orders for the destruction of unlawfully taken confidential information which is found in a search.

An example where such an application was successful is *AJG v Skriptchenko* [2016] EWHC 603 (QB), where a precise regime to identify the relevant documents was adopted: copies of all materials would be retained; any dispute as to whether material was confidential would be referred to the Judge; and, inspection and deletion was to be carried out by experts appointed by the defendants rather than the claimants, using agreed search terms. The Judge said he felt a high degree of assurance that the claimant would succeed at trial and also that the defendants could not be trusted to delete the material themselves. However, in light of *TBD (Owen Holland) Ltd v Simons*, *Skriptchenko* should now be regarded with considerable caution. In particular, it is submitted there was no good reason why the destruction needed to happen before the conclusion of trial, given that an image had been taken and the information had been deleted on the defendant's system.

Which side carries out the search?

Once an imaging order has been made on a 'without notice' application, the debate centres on what should be done with the images: who should be allowed to look at them first after filtering out privileged information? In *A v B; Hewlett Packard v Manchester Technology Data* [2019] EWHC 2089 (Ch), Mann J considered this issue after bringing together two cases which raised the same issue. One was an employee competition case. The other was a claim by HP that another company was selling counterfeit goods in their name. They wanted computer searches in order to show the full extent of the claim and also to consider taking action against other parties. After a review of the authorities, the Judge provided a detailed summary of the factors in play (which is further summarised here):

(i) The order will have been obtained the basis of a strong prima facie case of the dishonesty of the defendant but also the propensity of the defendant to cover his or her tracks by destroying evidence. That may mean that the defendant should not necessarily be trusted to carry out the disclosure (inspection) exercise properly. This factor may be seriously ameliorated by the defendant's solicitors being involved in the process.

(ii) The relevance of some important documents may be honestly missed by the defendant's solicitors.

(iii) It may be the case that urgency justifies the claimants carrying out the search. For example, it might be necessary, as a matter of urgency, to follow property, or to identify other wrongdoers in a supply chain.

(iv) Careful agreement of search terms might narrow the field to such an extent that the exercise becomes akin to the more familiar one of compelling disclosure of a class of documents, but which can be searched by the receiving party for relevance.

(v) It may be that the resources available to the claimant are greater than those available to the defendant so that it makes practical sense, in order to further the overriding objective, to allow the claimant to go first, though this must not be allowed to become a charter for the well-heeled to get an advantage.

(vi) Any digital image of the kind in issue in these cases is likely to contain irrelevant material which is private and confidential (if not privileged) and which should not, if it can be avoided, be seen by the claimant at all. *A v B* was a very good example. The business that the defendants carried on was in competition with the claimant. Even if they had confidential information of the claimant on their digital devices, there is also likely to be their own confidential information about their business which they would normally be entitled to keep confidential.

In *A v B*, the solution to dealing with these competing interests was to allow the defendant the first review for confidentiality and privilege (including mixed documents which contained one or other of those elements together with other material). The claimant could then search once confidential material had been removed, as they were better equipped to identify their own confidential information and there was some evidence the defendant could not be trusted.

Keyword searches

In *TBD (Owen Holland) Ltd v Simons* (CA), Arnold LJ provided an important qualification to Mann J's analysis by saying search terms "*must*" be agreed between the parties or determined by the court. Further,

"It is unacceptable for claimants to be able unilaterally to decide what keywords to employ, since experience shows that, as in this case, parties all too often propose keywords that are far too all-embracing. Considerable care is required when selecting keywords, and often it will be necessary for an intelligent combination of keywords to be employed. Furthermore, even careful keyword selection may not necessarily be an answer to the problem posed by privileged documents." (at [192])

Endorsing a more restrictive approach

Arnold LJ's robust guidance can be seen as the Court of Appeal's endorsement of a trend in some of the more recent cases towards a more restrictive approach to granting imaging and inspection orders, both on 'without notice' applications and more generally.

In *CBS Butler v Brown & Ors* [2013] EWHC 3944 (QB), the claimant, having already obtained an order for imaging of relevant storage devices for the purpose of "preserving" relevant evidence, made a further application seeking to allow its own IT expert to use keyword searches for disclosable material, whilst blacklisting search terms for information that should not be disclosed because of privilege. The Court refused the application. By the time of the hearing, a defence had been filed and disclosure would happen in due course. The order was "*intrusive*…

contrary to normal principles of justice," and could only be made "*when there is a paramount need to prevent a denial of justice to the claimant*."

CBS Butler v Brown demonstrates the restrictive approach. Whilst *Skriptchenko* and other first instance cases in the last few years had signalled a greater receptiveness to claimant-led inspection applications, even before the Court of Appeal's intervention, there were signs that the High Court was being more cautious in granting this type of relief.

An example is *Hi-Level Enterprises Ltd v Levine* [2018] EWHC 1882 (Ch), which gives a good example of how these principles might be applied in practice. The defendants had in principle accepted that there should be an order for inspection. The question for the Court was how intrusive the search should be. The claimant was proposing to carry out two searches: (i) to use specified search terms to see if any of the claimant's database remained on the delivered-up devices and whether the defendants had, as they asserted, tried to delete it; (ii) to identify whether any parts of a database belonging to the claimant, which had been copied by the defendant, had been transferred onto any devices of the defendants that had not been delivered up or disclosed.

The proposed first search was sufficiently specific and could be granted. However, the Judge accepted the defendant's objections to the second search: in particular, a provision in the proposed order that allowed the proposed specialist who was to carry out the search to 'take such sensible and proportionate steps to conduct the Search and Schedule A Search as is necessary' was impermissibly broad.

Post-script: Cost implications of an imaging and inspection order

An argument frequently raised by defendants is that these orders give rise to disproportionate and open-ended costs awards. In *Hi-Level Enterprises,* the defendant made a complaint about open-ended costs but the Judge considered that the claimant's acceptance of a cap of £10,000 for the inspection was an acceptable response to this contention.

Peter Linstead
Outer Temple Chambers
9 March 2021