MAYER·BROWN

Article

This article first appeared in a slightly different form in *Solicitor's Journal*, 11 January 2011

DOES CLOUD COMPUTING POTENTIALLY HINDER COMPLIANCE WITH DISCLOSURE OBLIGATIONS?

By Ed Sautter

Cloud computing involves the use of remote, internet-based, computing resources. The perceived advantage of cloud computing is the availability, on a pay as you go basis, of a virtually infinite infrastructure owned and managed by a third party and which does not, therefore, involve significant capital investment by the user.

It is likely that COO's and IT Directors will come under pressure from their businesses to consider the use of cloud computing but for those who are involved in risk management, and in particular are responsible for handling a company's response to litigation or to regulatory investigation or proceedings, what are the potential dangers of the company's data being held in the cloud?

When considering the position in relation to litigation, and, in particular, the requirement to provide disclosure of electronically stored information ("ESI"), CPR 31.8 requires disclosure of documents which are or have been in a party's control. Control for these purposes is defined as physical possession, a right to possession or a right to inspect or take copies of the documents in question. It has been suggested (see, for instance, Hollander on Documentary Evidence 10th Edition) that the test expounded in Lonrho v Shell [1980] 1 WLR 627 HL, a case decided under the pre-CPR regime, remains good law. The definition of "power" under those rules was that the disclosing party had a presently enforceable legal right to obtain the documents in question without the need for consent.

In the context of cloud computing a potentially significant issue is whether ESI held within the cloud would be treated for the purposes of the disclosure rules as being within the control of the user, even in circumstances where the user has in practice little or no say as to whether and, if so, how ESI is preserved and made available. ESI held within the cloud is likely only to be available through the cloud provider and the relevant provisions in the Service Level Agreement may not be sufficiently robust from the perspective of the user in order to ensure that all potentially relevant ESI can be identified, preserved and collected and, even if it can, in a form and within a timeframe consistent with the user's disclosure obligations. These potential issues are potentially exacerbated where relevant ESI is held within a shared public cloud; for instance, will it be possible to extract the relevant data separately from other users' data in the cloud? Further, in the case of fraud or similar circumstances, will the user be able to ensure that the collection is conducted in a forensically pure manner with all of the relevant metadata preserved? Again, what costs will the provider be seeking to levy for carrying out these processes?

A further potential issue concerns the location of the stored ESI. When a user purchases cloud computing services involving the processing and storage of data, it may not know where that data is actually held (i.e. the location of the servers on which the relevant processing and/or storage is conducted). Depending on the jurisdiction, such remote processing/storage

Ed Sautter

Partner, Litigation
esautter@mayerbrown.com

DOES CLOUD COMPUTING POTENTIALLY HINDER COMPLIANCE WITH DISCLOSURE OBLIGATIONS?

may inadvertently engage the data protection or similar rules of that jurisdiction. For instance, a US user of cloud computing services might find, if the relevant ESI is to be processed or stored within the EU, that the relevant ESI has become impressed with the processing and transfer restrictions of the European Data Protection Directive.

Consequently, in considering the utilisation of cloud computing services, careful consideration must be given to the terms of the Service Level Agreement in order to ensure (so far as possible) that the user has the right to access all relevant ESI on demand, in the required format and at a cost that is understood. Sufficient provisions should be drafted into the Agreement to ensure that the user can exercise sufficient control over the relevant ESI and contractually secure the co-operation of the cloud provider in implementing legal holds and collecting and producing ESI in a compliant manner. The user should also require transparency as to where the relevant ESI will be located so that it can, so far as possible, avoid data protection or similar issues. Consideration should also be given as to what indemnities the user might appropriately seek in respect of losses arising from failure by the provider to cooperate in ensuring that compliant disclosure is provided.

0340ldr
March 2011