EDITORIAL

The digital evidence specialist discovered that there were other attempts to communicate with the claimant's server from IP addresses registered to the defendant. This case illustrates the importance of digital evidence and also demonstrates that if digital evidence is not properly handled, its integrity can be damaged.

Two important issues have come to the fore over the past few months, both of which illustrate the importance that lawyers should attach to understanding digital evidence.

First, the damage that employees of an internal IT department can do to digital evidence in their ignorance cannot be over-estimated. This is illustrated in the case of *Aston Investments Limited v OJSC Russian Aluminium (Rusal)* [2006] EWHC 2545 (Comm). Aston alleged that the defendants hacked into their computer system in London in order to view confidential and privileged information in relation to litigation in which the parties are jointly engaged. A routine security scan of Aston's server revealed hidden spyware called 'Perfect Keylogger', installed at around 4 a.m. on 20 January 2006. The spyware was designed to make a log of everything typed on the computer, and take a snapshot of the computer screen and any information saved on file, which is then secretly transmitted to the person who installed it. An earlier version of the software was found on a computer operated by the receptionist and secretary, installed, depending on the dating system, either on 11 March or 3 November 2005. The domain user of the file was called 'Oroosinovich'. The spyware had been transmitting information to an internet address smtp.list.ru/194.67.23.115. An investigation established that a number of attempts had been made to gain access to the system from various IP addresses (one of which was an internet address registered to Rusal), several of which were successful. After taking this action, Ashton engaged a digital evidence specialist, who concluded that the actions of the members of the IT department had resulted in important files and information being removed, and a subsequent forensic examination of the original evidence was made very difficult because of changes made to the system. Indeed, the learned judge, Jonathan Hirst, QC, commented, at 43:

> *'As a result of the steps taken by Mr Sinani and Mr Makarov to prevent further unauthorised access, the alleged "crime scene" had been trampled over and any relevant foot prints were no longer discernible.'*

The digital evidence specialist discovered that there were other attempts to communicate with the claimant's server from IP addresses registered to the defendant. This case illustrates the importance of digital evidence and also demonstrates that if digital evidence is not properly handled, its integrity can be damaged.

The second issue relates to the cost of disclosure or discovery of digital documents. The Institute for the Advancement of the American Legal System at the University of Denver issued a joint paper with the American College of Trial Lawyers Task Force in September 2008, entitled 'Interim Report & 2008 Litigation Survey'. This survey makes it clear that there is a problem relating to electronic discovery in the United States of America. Four major concerns were identified:

1. Deserving cases are not brought because the cost of pursuing them fails a rational cost benefit test, while cases with no merit, especially smaller cases, tend to be settled rather than being tried because it costs too much to litigate them.
2. Discovery costs far too much and has become an end in itself.
3. Judges fail to take active control of litigation from the beginning. Where abuses occur, judges are perceived to be less than effective in enforcing the rules.
4. Local Rules are routinely described as 'traps for the unwary' and many think they should either be abolished entirely or made uniform.

This survey attracted the attention of *The Economist* (Technology, business and the law section) in an article entitled 'The big data dump' on 28 August 2008. Clearly, procedural rules governing disclosure or discovery are predicated upon cultural norms, as much as the legal philosophy of the State; the way litigation is conducted in the USA reflects the underlying philosophy of those responsible for the procedural rules, both at a Federal and State level. It is suggested, in the article from *The Economist*, that this is a US problem, and the following text offers the explanation:

> 'This is overwhelmingly an American problem. In countries such as France and Germany that have an inquisitorial legal

EDITORIAL

Perhaps litigants in many European States and the United States of America might prefer similar rules to that pertaining in England & Wales, where both sides have a duty to exchange a list of documents that are both in their favour and adverse to their case before trial.

> tradition, e-discovery tends to be proportionate to the case, because judges largely determine what information is relevant. By contrast, in adversarial common-law systems, it is the opponents in a case that decide how much information to peruse before picking out the evidence. But most countries within this tradition, such as Britain, Canada and Australia, have recently moved towards inquisitorial systems to minimise the threat from e-discovery.'

First, it is not an overwhelmingly American problem, although it can be said that the procedural rules of other States help to ameliorate the problems with digital evidence. The author of this article has failed to distinguish between criminal and civil proceedings, and puts all other States into the category of the 'inquisitorial legal tradition' as if such an alternative existed. Sweeping statements about inquisitorial legal traditions only serve to illustrate the want of understanding by the author.

Second, litigants in civil proceedings in France and Germany control the evidence that goes before a judge. Perhaps litigants in many European States and the United States of America might prefer similar rules to that pertaining in England & Wales, where both sides have a duty to exchange a list of documents that are both in their favour and adverse to their case before trial. The aim of this requirement is to ensure the trial only considers the issues in dispute. Peripheral issues of no relevance are not admitted. However, it may be that the English way is not persuasive: perhaps lawyers and litigants might prefer the rule in Malta, that allows the parties to produce documents during the course of the trial for the first time.

It must also be pointed out that countries such as Britain, Canada and Australia, have not moved towards inquisitorial systems. The basis of the author's opinion will be of interest indeed.

In essence, the problems relating to the disclosure or discovery of digital evidence face all lawyers in all States across the globe. It can be argued that a litigant wishing to initiate proceedings in a State where lawyers are hardly aware of the need to consider digital evidence in civil proceedings face just as serious a problem as in a State where lawyers are at least aware of digital evidence, even though the volumes of data are enormous.

Finally, a short note about the revised title of the journal. Previously entitled the *e-Signature Law Journal* and then re-named the *Digital Evidence Journal*, I have attempted to encourage people to understand that topics relating to digital evidence cover a vast range of devices and process, but to no avail. The new title is deliberately descriptive – to provide an international widow into the world of digital evidence and electronic signatures on a global scale – because this affects every lawyer in every country. The success of the journal is predicated upon lawyers and scholars taking part in the wider dissemination of knowledge, so please consider getting in touch if you have something original to share.

