EDITORIAL

Articles and cases will continue to be solicited and published about electronic signatures, and the new version of the journal aims to reflect the legal response to digital evidence in its widest forms.

The digital world is with us for the foreseeable future, and IT will continue to be used for nefarious purposes in ways that cover both the criminal and civil law. It is for lawyers and the IT industry to combine in order to more fully understand the nature of electronic, analogue and digital evidence, and it is also important to ensure proof of digital evidence is not sidelined into obscurity. Hence the change of name for the journal, to the *Digital Evidence Journal*. Articles and cases will continue to be solicited and published about electronic signatures, and the new version of the journal aims to reflect the legal response to digital evidence in its widest forms.

Some of the interesting issues that surround evidence in digital format include:

- Understanding the technical limitations in establishing integrity, and to consider what additional problems, if any, that new products and software may have on the nature of the evidence.
- Becoming more knowledgeable about the legal requirements from jurisdictions across the world in relation to the admission of digital evidence, how digital evidence is handled and treated in court, and the interpretation of legislation and procedures by judges, and how this affects the introduction of evidence between jurisdictions.
- The admissibility of digital evidence. Rules will shift across jurisdictions, the subject matter will change and the technology will constantly be up-dated.
- Examining the legal and 'scientific' notions of proof as applied to digital evidence of all kinds.
- Information system design that seeks to be evidentially 'sound'. Discussions of appropriate (or desirable) criteria when designing a system to be evidentially sound, that is, to provide documents, records and logs which are considered robust against questioning in the courts.
- Digital preservation and storage media is becoming a significant point of discussion for national archives.
- Forensic computing covers the admissibility of evidence obtained by a forensic examiner, problems relating to expert evidence (legal and practical), responses to novel scientific and technical evidence.
- What metadata is, the types of metadata, how metadata can be altered and the effect it can have on the weight of the evidence.
- Rules relating to disclosure or discovery in both civil and criminal procedure.

In addition, consideration should continue to be given to the future: trusted computing and data stored and encrypted by default are two issues of significance that recommend themselves for treatment, as does the more distant ubiquitous computing.

If you are interested in adding to the sum of knowledge with respect to digital evidence, please get in touch: this journal aims to be inclusive, not exclusive.

Electronic signatures

In the recent English case of *Mehta v J Pereira Fernandes S A* [2006] EWHC 813 (Ch), it was held on appeal that an e-mail address was not capable of being a form of electronic signature. Further details are in the news section of the journal, but two significant points arise from the initial appeal. First, judges should be encouraged to obtain expert opinion with respect to technical issues at an early stage of the proceedings. Second, if electronic signatures are going to be applied consistently across the world, the decisions of judges from other jurisdictions ought to be considered when such cases are brought before domestic adjudicators. For this reason, it is with sincere thanks to Michael G Rachavelias, the country correspondent for Greece, that a full translation of the Greek case *1327/2001 – Payment Order* is included in this issue of the journal.

Finally, this case has highlighted the need to consider a move to ensure decisions are readily available to judges in all jurisdictions in order to more fully understand the international framework within which they can be encouraged to make a decision. To encourage such international harmony, it cannot be beyond the realm of possibility that the United Nations and the major trading blocks, such as North America and the European Union, ought to be able to fund such an important initiative.

EDITORIAL

A significant question relates to the range of issues that might need to be considered when a party challenges the authenticity of a document in digital format.

The term 'authentic' is used to describe whether a document is genuine. However, it is, perhaps, misleading to use the term 'authentic' when referring to a digital document or, perhaps more accurately, a digital object. This is because of the way a digital object is created and made visible. For digital data to be made intelligible to a human being, it must be interpreted. Digital data is processed through a sequences of commands, so a simple document containing written text, for example, will consist of a number of ASCII character codes that must be interpreted before the text is reproduced on a screen in human readable format. However, digital data is not restricted to simple text documents. The format of the data can be of a more elaborate nature, including active components such as macros and scripting language, which means the data might require more complex interpretation to read the text. Also, a file displayed on a different computer to the computer that originally created the file, can, and often does, lead to a different font and different line breaks. This is why the format of a file of documents will differ.

The definition of authenticity in respect of a physical document comprise such attributes as the state of being the original, or of being faithful to an original, uncorrupted and, perhaps, with a verified provenance. In comparison, it is more difficult to be clear as to what is meant by an 'authentic' digital object. If, for instance, a particular macro (say a macro that is used to automate frequently used movements of the mouse) is missing from a computer upon which a copy of the digital document rests, the question that must be raised is whether the lack of the macro in the computer that the data now rests, renders the document something other than the genuine document.

To a certain extent, the technical focus of proving the authenticity of a digital object is to have checks and balances in place to demonstrate the history of how the data has been managed, which leads to the assertion that the data has not been modified, replaced, or corrupted and must, therefore, be 'original'. This proposition rests on two conditions: first, the data is subject to a chain of custody; and second, the data has not been modified without authority between the time it was created or added to the depository, to the moment it was required.

The unique nature of digital data means that although the data may be created in program memory, it might be saved on a number of different storage media. Further, each digital object may be replicated in a number of places, which means there is no single 'original'. This has implications for understanding the nature of digital data. In essence, there is a need to accept that the concept of an 'original' and 'authentic' digital object is meaningless. Therefore it is necessary to consider the meaning of 'authentic' in terms of a digital object in the relevant context. Conceptually, a digital object is authenticated by verifying the claims that are associated with the object, such as: the organizational criteria demonstrating the provenance of the digital object, including the documentation pertaining to the chain of custody (and what extent this documentation is trusted), and the extent to which the custodians can be trusted; the object can be examined forensically to establish whether its characteristics and content are consistent with the claims made about it and the record of its provenance; any signatures, seals and time stamps that may be attached to the object can help test the claims to consistency and provenance. In essence, the ability to prove the authenticity of a digital object is not proving that an original exists, especially when referring to something as dynamic as a database. The issue is about trust, or the lack of trust. Proving the authenticity of a digital object means providing sufficient evidence to convince an adjudicator that the object that has been retrieved is a faithful representation of what is claimed to be the 'original,' or a reliable representation of the object that was in turn relied upon by the originator.