EDITORIAL

The source of the leak could only be the result of two possibilities, and CAAT did attempt, unsuccessfully, to trace the source, as described by Mr Justice King

The nature of the problems lawyers will continue to face respecting digital evidence is illustrated in the recent case of *Campaign Against Arms Trade v BAE Systems PLC* [2007] EWHC 330 (QB). Mr Justice King granted Norwich Pharmacal relief to the Campaign Against Arms Trade (CAAT) against BAE Systems PLC (BAE) in this instance. Ann Feltham sent an e-mail on the 29 December 2006 to the members of the CAAT steering committee internal e-mail list (caatcommiteee@lists.riseup.net), a private list not open to the members of the public and comprising only the 12 members of the steering committee and seven members of CAAT's staff. The e-mail contained privileged legal advice that CAAT received from its solicitors. A copy of the e-mail was sent to BAE. Solicitors for BAE returned a copy of the e-mail printed on paper to CAAT's solicitors. This was the first time that CAAT came to know of the leak.

The e-mail returned to CAAT was incomplete, as described by Mr Justice King, at 31:

> 'It was a redacted version of that which had come into the possession of the Respondent and/or its own solicitors. All the routing information, the header address and so forth, which would give details of the email accounts through which the email had been received and sent before arriving at the Respondent and its solicitors, had been removed. Such removal must have been done either by the Respondent or by its solicitors acting on its instructions.'

The source of the leak could only be the result of two possibilities, and CAAT did attempt, unsuccessfully, to trace the source, as described by Mr Justice King:

> '45. As Ann Feltham says, there are really only two broad possibilities: either the source is one of the authorised recipients of the email, i.e. a member of the Applicant's steering committee or staff, or the email was intercepted or retrieved by other means by a person or persons unknown, be it by improper access to the Applicant's or a recipient's computer system, interception at riseup.net or at some point whilst the email was sent over the internet. In her first witness statement she explains how she made enquiries of each of the authorised recipients who each denied forwarding the email on. Her second witness statement was made in response to that part of the Respondent's skeleton argument in which it is said that the Applicant has not done enough and that before seeking the present order the Applicant should have (skeleton para.27.) "examined the electronic data available to it on its own computer systems and those of 'riseup.net' and further should have asked any authorised recipients to provide it with access to their personal electronic data for purpose of determining whether their denials of involvement in the copying are accurate".
>
> 46. In this later statement Ms Feltham says she did check the 'sent folders' on the personal computers of the staff based in the Applicant's office, but explains that there was a major practical and logistical problem as regards access to the computers used by members of the steering committee. Unlike the staff they are not employees of the Applicant but volunteers who do not work in the office or use computer systems belonging to the Applicant. Some are members of other organisations who access emails from accounts and equipment owned by their employers. Some are based outside London. This all means that to have investigated further on the lines suggested by the Respondent, the Applicant would have needed access to computers to which the Applicant has no right of access and in any event the Applicant would have needed the "costly services of a computer expert to go on a fishing expedition for emails which might or might not have been sent which moreover would have been very time consuming.'

The claim by BAE that CAAT ought to physically examine every computer to trace the route of the e-mail is somewhat unrealistic, as explained above, and also fails to grasp the fundamental issue, that digital data knows no geographical, physical bounds. Returning the e-mail without the source data is similar to returning a letter received through the post in an envelope, yet refusing to deliver up the envelope. That the routing and other technical data is 'similar' to the data included on an envelope is an understatement, because the routing and other metadata available in relation to an e-mail is far more extensive than the metadata contained on an envelope. In this instance, Mr Justice King concluded that the order sought ought to be granted, although not in the terms requested.

This application, and the decision by Mr Justice King, illustrates the importance of the metadata associated with a digital object. Documents in digital format include metadata as a matter of course, and it seems unrealistic for the recipient to refuse to deliver up the full document, including the associated metadata, in such circumstances.

EDITORIAL

Unless legal academics educate potential lawyers in digital evidence, and judges and lawyers concern themselves with the need to be educated in the topic, more rough justice can be expected across the globe.

The introduction of paper caused some lawyers consternation in Europe, mainly because lawyers did not know how to assess the veracity of the contents recorded on the paper carrier. As a result, elaborate rules were developed in some countries for the authentication of documents recorded on paper so as to prevent or counter attempts at fraud. At the time, the pace of change was probably slow enough to ensure that lawyers, judges and those that entered the profession were able to improve their knowledge and understanding of the evidential requirements relating to the introduction of paper relatively easily.

However, some centuries later, a similar change *has already taken place* with respect to digital data, and, it seems, that a large majority of lawyers, legal academics and judges have failed to realize they are now living in a world dominated by digital evidence, *and that digital evidence is now the dominant form of evidence.* Although quantifiable figures are not available, it can be asserted with some confidence that the majority of lawyers, legal academics and judges do not know they do not know; a smaller number know they do not know, and an even smaller elite know about digital evidence, but they are realistic enough to know they need to know more.

The law acts as a means to provide for social stability, yet if lawyers and judges fail to grasp that they need to begin to understand the attributes of evidence in digital format, individuals that are caught up in events such as those illustrated in the case of the *State of Connecticut v Julie Amero* (January 2007, Docket number CR-04-93292, Superior Court New London Judicial District at Norwich, GA 21) will find themselves subject to the collective failure of the legal system: by the prosecution, defence and judge. This failure to become familiar with evidence in digital form by the participants in the legal system is further acerbated by the failure of the majority of universities and law schools across the world to incorporate any discussion of digital evidence into the curriculum. This means that the majority of students are taking degrees and participating in vocational training that ignores the new reality, that virtually all evidence brought before a court within the next three years will be from a digital source (see *The Expanding Digital Universe: A Forecast of Worldwide Information Growth Through 2010* (IDC White Paper, March 2007). Yet the vast majority of students, lawyers and judges do not know how to assess such evidence, nor are they in a position to brief digital evidence specialists effectively, or to ask the right questions of such specialists during the legal proceedings.

This state of affairs will continue for some time, and it seems probable that many people brought before a criminal court may well face rough justice if the digital evidence is misunderstood by the lawyers and judge alike. In addition, parties in civil proceedings may also face serious obstacles if their lawyers and the judge fail to understand the importance of digital evidence: one European lawyer informed the editor this summer that they witnessed a judge refuse to receive photographic evidence taken on a mobile telephone of the damage caused to a motor car by another driver because, the judge asserted, the evidence could have been fabricated – there was not even a discussion as to the burden of proof or the procedure relating to which party could call into question the authenticity of the photographs – the judge blankly refused the admission of the evidence.

At the other end of the continuum, United States Magistrate Judge Paul W. Grimm in *Lorraine v. Markel and American Insurance Co* 2007 ILRWeb (P&F) 1805, 207 WL 1300739 (D. Md. May 4, 2007) provided a useful academic paper on the authentication of digital evidence, yet failed to indicate why he decided to dismiss certain evidence because it was not authenticated.

Unless legal academics educate potential lawyers in digital evidence, and judges and lawyers concern themselves with the need to be educated in the topic, more rough justice can be expected across the globe. Not only rough justice. Lawyers in some jurisdictions can expect to face actions for negligence: this will then cause the professional indemnity insurers to take notice, and lawyers will then rush to become more educated. In the meantime, it is only to be guessed how many lay clients will be at the receiving end of poor legal advice in respect of digital evidence.