

# Preface

Lawyers and judges now deal with digital evidence regularly, even if it is mainly in the form of email correspondence, the authenticity of which may not be in question. The short list of random examples cited below illustrates how many, and how varied, the sources of digital information are, and the purposes to which the evidence is put. Email has become ubiquitous and is now cited regularly in evidence across a range of civil and criminal cases, including allegations of defamation<sup>1</sup>; messages left on mobile telephone voicemail facilities have been tapped and subsequently misused in at least one case in England and Wales<sup>2</sup>; fugitives have been tracked down when using a Skype telephone<sup>3</sup>; a pastor has used text messages to incite his lover to murder his wife<sup>4</sup>; a professor has used the internet to search for the means to kill his ex-wife<sup>5</sup>; Khalid Shaikh Mohammed, accused of being the mastermind of the attacks in the USA on 11 September 2001, was arrested because he, together with his accomplices, used the same the SIM card in whatever mobile telephone they used, thus enabling the security services across a number of continents to track the use of the card<sup>6</sup>; evidence from the global positioning

- <sup>1</sup> *Western Provident Association Ltd v Norwich Union Healthcare Ltd and Norwich Union Life Insurance Co Ltd* (1997) *Financial Times*, 18 July, (1997) *The Times*, 18 July; *Exoteric Gas Solutions Ltd and Andrew Duffield v BG plc* [1999] LTL 24 September 1999, (1999) *The Independent*, 24 June; *Takenaka (UK) Ltd and Corfe v Frankl* [2001] EWCA Civ 348, [2001] EBLR 40. Comments placed on web sites have also been the subject defamatory proceedings: *Jim Murray v Spencer, Steve and Pankhurst*, see 'Friends Reunited user pays damages' (2002) *BBC News*, 21 May, available online at [http://news.bbc.co.uk/2/hi/uk\\_news/england/1999231.stm](http://news.bbc.co.uk/2/hi/uk_news/england/1999231.stm) and an OFCOM Adjudication on a related matter: [http://www.ofcom.org.uk/tv/obb/prog\\_cb/pcb\\_15/f\\_p/adj\\_jm.pdf](http://www.ofcom.org.uk/tv/obb/prog_cb/pcb_15/f_p/adj_jm.pdf); and for comments placed in chat rooms: *Michael Keith-Smith v Tracy Williams*, see Adam Sherwin 'Chat room insults lead to internet libel victory' (2006) *The Times*, March 22, available online at <http://www.timesonline.co.uk/article/0,,2-2097470,00.html>; Owen Gibson 'Warning to chatroom users after libel award for man labelled a Nazi' (2006) *Guardian Unlimited*, March 23, available online at <http://www.guardian.co.uk/law/story/0,,1737445,00.html>.
- <sup>2</sup> *Relf v Rifkind; Hibbert v Rifkind* [2002] EWHC 2199 (Ch).
- <sup>3</sup> Eric Bangeman 'Fugitive exec nabbed after Skype call' (2006) *Ars Technica* 24 August, online at <http://arstechnica.com/news.ars/post/20060824-7582.html>.
- <sup>4</sup> 'Murderous texts send pastor to jail' (2004) *Reuters*, 3 August, archived by WorldWide Religious News online at <http://www.wwrn.org/article.php?idd=7133&sec=71&con=48>.
- <sup>5</sup> Stacey Archambault and Jaime Pedigo 'Murray found guilty of murder' (2005) *KUJH-TV News* March 17, online at <https://tv.ku.edu/news/2005/03/17/murray-found-guilty-of-murder>; Jesse Manning 'Murray convicted of murder Jurors return guilty verdict following 3 days of deliberations' (2005) *Kansas State Collegian*, March 18, online at <http://collegian.ksu.edu/collegian/article.php?a=5466>.
- <sup>6</sup> Don Van Natta Jr and Desmond Butler 'How Tiny Swiss Cellphone Chips Helped Track Global Terror Web' (2004) *The New York Times*, March 4, online at <http://>

## Preface

device placed on a vehicle was admitted into the trial of the murder of Scott Peterson's wife and their unborn son<sup>7</sup>; Blake Ranking confessed on a blog to causing a car to leave the road, and subsequently entered a plea of guilty to manslaughter<sup>8</sup>; email correspondence helped the police find the person alleged to have killed Bobbie Joe Stinnet and remove the baby she was carrying from her womb—Lisa Montgomery had communicated with the victim by an exchange of instant messages and emails, which enabled the police to locate her through the IP address<sup>9</sup>; evidence of a video taken on a mobile telephone of a woman performing a 'lap dance' whilst naked saved three men from being tried for rape, and subsequently caused the alleged victim, Cinzia Sannino, to enter a plea of guilty to two charges of perverting the course of justice<sup>10</sup>; the trial of a Kurdish youth was dismissed when he played a recording of the comments made by the arresting officer, PC David Yates of the Territorial Support Group of the Metropolitan Police, the recording was made on his mobile telephone at the time he was arrested (PC Yates used abusive language to allege the youth was a robber and a rapist, was subsequently charged with a racially aggravated attack on a Kurdish man and found not guilty at a trial held at Southwark Crown Court in January 2007)<sup>11</sup>; digital evidence from a wide variety of sources demonstrated how Dhiren Barot planned to initiate a number of terrorist attacks in London and the United States—the evidence was so overwhelming, that he entered pleas of guilty to the charges<sup>12</sup>; allegations of industrial espionage by the use of 'spyware' will be considered by the High Court in London when the trial takes place in the dispute between Ashton Investments and Ansol against Rusel Management Company and others<sup>13</sup>; and in the divorce action of *White v White*<sup>14</sup>, the husband failed in his application to have email correspondence suppressed on the basis that his wife unlawfully intercepted the email and intruded upon his privacy by looking through his files on the computer: *Issenman JSC* held that merely looking through files stored on a computer used by all members of a family

[www.nytimes.com/2004/03/04/international/europe/04PHON.html?ex=1393736400&cen=71c64fa22f23d30a&ei=5007&partner=USERLAND](http://www.nytimes.com/2004/03/04/international/europe/04PHON.html?ex=1393736400&cen=71c64fa22f23d30a&ei=5007&partner=USERLAND).

<sup>7</sup> 'Peterson Trial: Judge Allows In GPS Technology Evidence' (2004) *Foxreno.com* February 27, online at <http://www.foxreno.com/news/2853360/detail.html>; Diana Walsh, Stacy Finz and Kevin Fagan 'Jury recommends death for Scott Peterson 11 hours of sentencing deliberations cap six-month trial' (2004) *San Francisco Chronicle*, December 13, online at <http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2004/12/13/PETERSON13.DTL>.

<sup>8</sup> 'Teen pleads guilty after blog confession' *MSNBC.com* online at <http://www.msnbc.msn.com/id/10561564/>.

<sup>9</sup> 'Web Led Cops To Stinnett Suspect' (2004) *CBS News* December 21, online at <http://www.cbsnews.com/stories/2004/12/21/national/main662366.shtml>.

<sup>10</sup> Simon De Bruxelles ' "Evil" teenager who cried rape is jailed' (2006) *The Times*, September 19, p 16.

<sup>11</sup> 'Officer suspended in racism probe' (2005) *BBC News*, 19 May, online at <http://news.bbc.co.uk/1/hi/uk/4561131.stm>; 'Policeman denies "racist attack"' (2006) *BBC News*, 5 April online at <http://news.bbc.co.uk/1/hi/england/london/4879946.stm>; 'PC Suspended After Racist Rant' (2005) *Muslim Directory*, 8 June online at <http://www.muslimdirectory.co.uk/viewarticle.php?id=40>; 'Officer not guilty of race attack' (2007) *BBC News*, 31 January, online at <http://news.bbc.co.uk/1/hi/england/london/6317751.stm>.

<sup>12</sup> Sean O'Neill and Adam Fresco ' "Dirty" bomber's plot to hit stations and hotels' (2006) *The Times*, November 7, pp 1 and 6.

<sup>13</sup> *Ashton Investments Ltd v Rusal Management Co* [2006] EWHC 2545 (Comm).

<sup>14</sup> 344 N.J. Super 211, 781 A.2d 85 (N.J. Super. Ch. 2001).

did not constitute an act of interception and that the wife had an equal right and authority to view files on the computer in the same way as the other authorised users.

As the examples set out above illustrate, lawyers handle digital evidence every day, even though the vast majority of them are not aware that they do so. It is partly for this reason that this book has been written. The main aim of the text is to offer judges, lawyers, legal scholars and students an insight into the complexities of electronic evidence in its widest sense. For this reason, the content of the book sets out in brief the sources of digital evidence; identifies the characteristics of digital evidence; considers the issues involved with the investigation and reporting of digital evidence; discusses the evidential foundations for adducing digital evidence into legal proceedings; sets out and explains the use of animations and simulations using computers; and individual chapters put the admissibility of electronic evidence in each jurisdiction into context, placing electronic evidence into the framework that is familiar to participants in the justice system. For lawyers, it is hoped that this text will provide useful guidance that is sufficient to enable them to begin to understand what questions to ask of digital forensic specialists and to advise on electronic evidence confidently, competently and with assurance. It is also thought that the text may be of interest to law enforcement agencies, digital forensic specialists and the IT industry in general.

To further illustrate the nature of the topic, weeks before the publication of this text, Mr Justice King granted Norwich Pharmacal relief to the Campaign Against Arms Trade ('CAAT') against BAE Systems plc ('BAE')<sup>15</sup>. Ann Feltham sent an email on the 29 December 2006 to the members of the CAAT steering committee internal email 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 email contained privileged legal advice that CAAT received from its solicitors. A copy of the email was sent to BAE. Solicitors for BAE returned a copy of the email printed on paper to CAAT's solicitors, by a letter dated 9 January 2007, received the following day. This was the first time that CAAT came to know of the leak.

The email 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

<sup>15</sup> *Campaign Against Arms Trade v BAE Systems plc* [2007] EWHC 330 (QB).

## *Preface*

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 email is somewhat unrealistic, as explained above, and also fails to grasp the fundamental issue: that digital data knows no geographical, physical bounds. Returning the email 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 email 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.

The mix of common law jurisdictions included in this book serves to demonstrate that the same or similar problems occur in every jurisdiction. In planning the book, an outline of the topics was agreed (although this was subsequently amended as work progressed), subject to the different nuances peculiar to each jurisdiction that inevitably meant each author took a slightly different approach. The resulting text does not have a uniformity about it that might please the legal aesthete. In addition, the chapter on England & Wales is of much greater length than the other chapters, at the request of the publisher, although it is the editor's wish and intention to encourage the contributors of country chapters to expand on their treatment in future editions. It is for this reason that the reader is invited to offer comments regarding the usefulness or otherwise of the text so that, when future editions are planned, consideration can be given to suggestions from readers.

To summarise, evidence in a digital format fits into a number of categories:

- (a) records of activities that contain content written by one or more people. Examples include email messages, word processing files and instant messages. From an evidential point of view, it may be necessary to demonstrate that the content of the document is a reliable record of the human statement that can be trusted;
- (b) records generated by a computer that have not had any input from a human. Examples of such records are data logs, connections made by telephones, and ATM transactions. The main evidentiary issue with such records may be to demonstrate that the computer program that generated the record was functioning properly at the material time;
- (c) records comprising a mix of human input and calculations generated and stored by a computer. An example is that of a financial spreadsheet that contains human statements (input to the spreadsheet program) and computer processing (mathematical calculations performed by the spreadsheet program). From an evidential point of view, the issues are whether the person or the computer created the content of the record, and how much of the content was created by the computer and how much by the human. It is possible that the input could be hearsay and that the authenticity of the computer processing might be in issue.

It is possible to challenge the authenticity of digital evidence in a number of ways, although many reported cases appear to indicate that a lawyer will merely assert that the authenticity or reliability of the evidence is not to be trusted, and the court will then have to determine a suitable response to the allegation raised. Digital evidence can be challenged in a number of ways:

- (a) it may be claimed that the records were altered, manipulated, or damaged between the time they were created and the time they appear in court as evidence;
- (b) the reliability of the computer program that generated the record may be questioned; and
- (c) the identity of the author may be in dispute: the person responsible for writing a letter in the form of a word processing file may dispute they wrote the text or, alternatively, it might be agreed that an act was carried out and recorded but at issue could be whether the person alleged to have used their PIN, password or clicked the 'I accept' icon was the person that actually carried out the action.

Finally, the vast range of information that is now available to lawyers can be helpful but, because of the sheer volume, difficult to manage. In England and Wales the system of justice is dependent on the assistance given by advocates to the court and advocates are required to bring relevant authorities to the attention of the court. The members of the Court of Appeal in the case of *Copeland v Smith*<sup>16</sup> had occasion to address this issue when it became apparent that a relevant authority had not been brought to the attention of the court, which meant it was assumed the judge could rule on a matter in the

<sup>16</sup> [2000] 1 WLR 1371.

## *Preface*

absence of any authority. Research carried out by both instructing solicitors and counsel failed to uncover a relevant authority. This was commented upon by Buxton LJ at 1372–1373:

‘I cannot draw back from expressing my very great concern that the judge was permitted by those professional advocates to approach the matter as if it were free from authority when there was a recently reported case in this court directly on the point, which was reported not in some obscure quarter but in the official law reports. It is, of course, not only extremely discourteous to the judge not to inform him properly about the law, but it has also been extremely wasteful of time and money in this case ... I have, I fear, to say that the advocates who appeared below did not discharge their duty properly to the court in that they apparently failed to be aware of the existence of that authority.’

In his judgment, Brooke LJ made a number of observations respecting the introduction of the new Civil Procedure Rules then, at 1375–1376, addressed the point made by Buxton LJ:

‘In these circumstances it is quite essential for advocates who hold themselves out as competent to practice in a particular field to bring and keep themselves up to date with recent authority in their field. By “recent authority” I am not necessarily referring to authority which is only to be found in specialist reports, but authority which has been reported in the general law reports. If a solicitors’ firm or barristers’ chambers only take one set of the general reports, for instance the Weekly Law Reports as opposed to the All England Law Reports, or the All England Law Reports as opposed to the Weekly Law Reports, they should at any rate have systems in place which enable them to keep themselves up to date with cases which have been considered worthy of reporting in the other series. If this is not done, judges may be getting the answer wrong through the default of the advocates appearing before them.’

Not only is it not in the interests of the system of justice that a relevant authority is missed but it cannot be in the interests of the client to miss a relevant authority (or authorities) when making submissions on their behalf before a court. There is a serious point to the comments made by the members of the Court of Appeal in the context of electronic evidence. The comments made by Brooke LJ inferred that the advocate that holds themselves out to practice in a particular field ought to be aware of recent authorities in that field. However, evidence in electronic format covers all areas of law and this means that every lawyer should make themselves aware of the nature and complexities of electronic evidence, because it is no longer a specialist area of legal practice, if ever it really was.

This text aims to help everybody involved in the justice system, either by reinforcing the strengths of their knowledge or, where they have no knowledge, to recognise the need to begin to understand the nature of the world they now inhabit before an action for negligence hits their in-box. If this book achieves either of these aims it will have justified the time spent in preparation.

*Stephen Mason*  
Langford, Bedfordshire  
February 2007  
stephenmason@stephenmason.eu