



eDisclosure: Lawyers are Treading a Risky Path

February 2007

Authors: Alan Phillips (7Safe), James Kent (7Safe)

Technology is moving fast; perhaps too fast for some. Fifteen years ago, lawyers were not hampered with the masses of evidence that result from email, instant messenger chat logs, spreadsheets and the like. We worked in a world of paper documents; it was straightforward, everyone knew the system and it had been that way for years.

Things then rapidly changed. The world's richest people were no longer oil sheikhs but mild mannered, bespectacled nerds. The time of the techies had come, and with it, the data explosion. Today, if a new PC's hard drive were to be full of text documents, printing them all could result in a stack of paper equivalent to the height of Mount Everest.

In a litigation case, lawyers have a method of getting around that problem; they politely ask for each clients' relevant documents and examine them using keyword searches. What would happen if they found out that the evidence collected in the case had been retrieved in an unreliable way? What if there were further, potentially crucial documents that existed that they would never know about? Would they know if the documents they had in their possession had been tampered with?

Digital evidence can be very compelling. Because people are often much less careful in email exchanges than they might be when composing a letter that is printed on the corporate stationery, it can be an especially valuable source of evidence in litigation. There are, however, many other avenues that can yield useful digital evidence.

In reference to a recent criminal case in which a man was strangled on the way home from his local drinking establishment, there seemed to be no obvious motive. Some DNA trace was retrieved from his neck area and the police requested that family and friends voluntarily provide a sample of theirs to eliminate them from enquiries. They duly obliged but the deceased's brother-in-law declined the request, and then hastily agreed after realising that he had become the prime suspect. The DNA exercise proved fruitless because on the night of the murder heavy rain had washed much of the trace evidence away and consequently there was not enough to give a positive match.

The brother-in-law's computer was seized as the investigation continued. In doing so, standard procedure best practice guidelines which are recognised in every criminal court in the UK were followed. A computer forensic specialist searched the suspect's machine and discovered that on the day before the murder, he had typed into an Internet search engine the following:

How to kill a man

This simple yet damning digital evidence proved to be significant in solving the crime. Yet, if it had been handled in the way that electronic evidence is treated in many civil litigation cases, it would have been unequivocally dismissed. How did the police's computer forensic expert know how to take the correct steps to ensure its admissibility? Simple - The criminal justice system is way ahead of the game.

High standards have been set by law enforcement agencies worldwide. In the UK, the de facto ACPO¹ Good Practice Guide to Computer Based Evidence is followed by computer forensic practitioners.

Is Ignorance Bliss?

Meanwhile, some lawyers readily accept documents which have been 'dragged and dropped' onto a CD burned by their clients, no questions asked. It's not their fault, though. Those lawyers and their clients have never been taught the 'evidentially sound' way to do things. And would anyone else involved in a civil case know any different? Perhaps not to date, but it's only a matter of time before the impact of this hits.

And it could hit hard, perhaps challenging every ruling where evidence has been similarly mishandled.

It might be coming soon to a case involving you. A recent survey² revealed that 15 percent of companies have gone to court to battle lawsuits triggered by employee email alone. American courts are heading in the right direction. In December 2006, the case of **Ameriwood Industries., Inc v Liberman** continued the inevitable march towards acceptable computer forensic practices in the United States³.

The plaintiff, Ameriwood, alleged that its former employees (and their recently formed company) used Ameriwood's computers and confidential information regarding its business, and defendants' positions of trust and confidence while in plaintiff's employ to sabotage plaintiff's business relationships and divert plaintiff's business to themselves.

Ameriwood sought production of "All computer or portable or detachable hard drives, or mirror images thereof, used by Liberman, Fridley, or Kleist since May 2005, including but not limited to any computer or portable or detachable hard drives in their homes."

The court stated that Ameriwood had argued that its former employees forwarded customer information and other trade secrets from Ameriwood's computers to defendants' personal email accounts, and that the documents may have been further disseminated to others and/or deleted to hide defendants' actions. Defendants argued that the requested information had already been disclosed and that they had not refused to search through their electronically stored information for such communications.

The court sided with Ameriwood, noting that some electronically stored information might not be obtained during a typical search. It explained:

Computer programs may retain draft language, editorial comments, and other deleted matter (sometimes referred to as 'embedded data') in an electronic file but not make them apparent to the reader. Information describing the history, tracking, or internal management of an electronic file (sometimes called 'metadata') is usually not apparent to the reader viewing a hard copy or a screen image.

Further, the court cited an email filed by plaintiff, which had been sent by one of the former employees to Samsung, a customer of plaintiff, while the employee was still in plaintiff's employ. Ameriwood asserted, and defendants did not dispute, that defendants had not produced it. The court concluded:

In light of the Samsung email, the Court found that other deleted or active versions of emails may yet exist on defendants' computers. Additionally, other data may provide answers to plaintiff's other pertinent inquiries in the instant action, such as: what happened to the electronic files diverted from plaintiff to defendants' personal email accounts; where were the files sent; did defendants store, access or share the files on any portable media; when were the files last accessed; were the files altered; was any email downloaded or copied onto a machine; and did defendants make any effort to delete electronic files and/or 'scrub' the computers at issue.

The court next evaluated whether there was good cause to allow plaintiff to obtain mirror images of defendants' hard drives. The court concluded that, considering the close relationship between plaintiff's claims and defendants' computer equipment, and having cause to question whether defendants had produced all responsive documents, it would allow an independent expert to obtain and search a mirror image of defendants' computer equipment.

The court set out an elaborate three-step imaging, recovery, and disclosure process, which was intended to provide the requesting party sufficient access to information that was not reasonably accessible, and to ensure the process did not place an undue burden on the responding party. Further, since Ameriwood did not object to incurring the costs for the requested procedures and defendants did not perform the procedures in the regular course of their business, the court ordered that Ameriwood would incur the costs involved in creating the mirror images, recovering the information, and translating the information into searchable formats.

The ACPO Good Practice Guide contains four 'Principles of Computer Based Electronic Evidence' designed to cover all computer based evidence, including eDisclosure cases:

Principle 1: No action taken should change data held on a computer or storage media which may subsequently be relied upon in court.

This requirement may seem straightforward but it isn't. The integrity of digital evidence is easily compromised if handled incorrectly, so specialist hardware, software, training and experience all need to be utilised to ensure that evidence is correctly captured in the first place.

Even the simple act of powering up or shutting down a machine causes changes to be made to many files on a computer's hard drive. Copying emails or Word documents to a CD can cause the loss of or change to extremely important metadata⁴ but the implications of mishandling electronic evidence are not obvious because these changes go on behind the scenes and thus do not appear in printed copies of the documents.

Just think what changes your client's IT department can innocently make whilst they diligently look for relevant information in a litigation case, such as accessing, deleting or changing vital information. Such changes may also not be so innocent, as altering electronic documents and their accompanying metadata is easily achieved.

The ultimate solution is to make an exact 'mirror image' of the media (e.g. hard drives) because it maintains the integrity of any evidence that may be later relied upon. This includes data that has actually been deleted (yes, beyond the recycle bin), another potentially massive benefit that is clearly sought in *Ameriwood Industries v Liberman*.

To ensure that the data on the mirror image is not altered in any way during the imaging process, hardware known as a 'write blocking' device is used. An integrity check is made to verify that the original hard drive and mirror image hard drive are exactly the same. Once a mirror image has been made it is effectively a preserved snapshot, frozen in time.

Don't assume that your clients will know about or have the in-house ability to cope with these procedures. Generally, even most IT departments brimming with übergeek techies do not have the tools or knowledge required to perform the operations described above.

Principle 2: In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, the person must be competent to do so and able to give evidence explaining the relevance and the implications of their actions.

In many eDisclosure cases exceptional circumstances are likely to be the rule rather than the exception, as documents will be collected from live, running servers that need to remain continually operational in a business setting. However, this is not the get-out clause that you may have been hoping for, as the circumstances referred to still require evidence from an expert.

Principle 3: An audit trail or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

This principle is of paramount importance, and is only workable if standardised best practice evidence collection and analysis procedures are agreed upon and strictly adhered to. Clearly, this does not currently happen in the majority of eDisclosure cases.

The final principle is fairly self-explanatory:

Principle 4: The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

Other best practice guides exist⁵, and they are virtually identical to the guide produced by ACPO.

In some cases the proportional costs involved will no doubt be a bone of contention, but the question must be asked: If electronic evidence has not been correctly handled in the initial stages, isn't the entire case inherently flawed from then onwards? Not following the evidentially sound guidelines could therefore prove to be much more costly.

There is a massive up side to all of this. Once the legal fraternity embraces best practice and realises the potential of what can be achieved with digital forensics, eDisclosure and many other types of cases could take very different twists.

A sample of what digital forensic experts are able to do using a robustly documented, evidentially sound process:

- Use many types of data can be useful as evidence, such as calendar files, web sites visited (and search engine phrases typed), instant messenger logs, spreadsheets, images, audio files, malicious software as well as old favourites emails and word processing documents
- Fraudulent document alteration detection (e.g. metadata edits)
- Recovery of deliberately (or otherwise) deleted documents
- Find evidence of attempts (successful or unsuccessful) to permanently erase or 'scrub' data from hard drives
- Utilise evidence from additional, commonly used devices holding communications data such as mobile phones and personal digital assistants (PDAs)

In this field, knowledge is power. Unless lawyers ensure that eDisclosure data is collected in an evidentially sound manner they are increasingly likely to be confronted by another lawyer who will challenge them and win.

About the authors

Alan Phillips (MBCS) is Managing Director at 7Safe, a firm specialising in digital forensic investigations. Alan is a member of the British Computer Society's Information Security Specialists Group and a founding member of the Institute of Information Security Professionals.

James Kent (CFIA) is Head of Technology at 7Safe Limited. James is an experienced digital forensics practitioner, registered expert witness and teacher of digital forensics to Masters level.

¹ Association of Chief Police Officers

² 2006 Workplace E-Mail, Instant Messaging & Blog Survey

³ Case summary information paraphrased from 'Court Orders Mirror Imaging of Defendants' Hard Drives and Sets Out Three-Step Imaging, Recovery, and Disclosure Process' from www.klgates.com

⁴ Information relating to the document itself such as creation, last modified and accessed date and times

⁵ For example, The G8 Proposed Principles For The Procedures Relating To Digital Evidence