

DIVIDED (AGAIN) BY A COMMON LANGUAGE: ELECTRONIC DISCOVERY (DISCLOSURE) IN THE U.K.

By Sharon D. Nelson, Esq. and John W. Simek

© 2008 Sensei Enterprises, Inc.

The English and the Americans have long been divided by a common language. We chortle when the English call trash cans “wheelie bins” or ask for a rubber (eraser). We can’t even get past the first question about electronic discovery without being gently reminded that, in the U.K., it is electronic disclosure, not discovery. We didn’t get past the second question without being told politely that the correct term in the U.K. is forensic computing, not computer forensics. We were gravely told that “forensic” is an adjective, not a noun, and humorously chided for yet another example of the Yanks getting things bollixed up again. We are still sometimes affectionately regarded as “the colonies” in Britain.

We ventured to London to seek the thoughts of those involved in electronic disclosure in the U.K., to ascertain both the similarities and the differences between the two countries. In our quest, we were aided greatly by the generous assistance of those we interviewed, representing a cross-section of folks involved what we called EDD for short, which allowed us each to translate to Electronic Data Discovery or Electronic Data Disclosure in accordance with our countries of origin.

The experts we interviewed included Laurie Watt (Senior Counsel) and John Sykes (Partner) from the law firm Charles Russell, Darren Pauling (Forensic Tech Director Operations) and Rahoul Bhansali (Senior Manager, Forensic) from KPMG, Adrian Palmer (Director) from Palmer Legal Technologies, Ian Henderson (President) from Advanced Forensics, and Dr. Ian Mitchell and Dr. Carlisle George (Senior Lecturers in Forensic Computing) from Middlesex University.

Is the U.K. or the U.S. more advanced in computer forensics and EDD?

There was general agreement that while electronic evidence came to the forefront at roughly the same time in the U.K. and the U.S., the U.S. is now the acknowledged leader in computer forensics and EDD, largely for two reasons:

- 1) The British are simply less litigious and so there are few cases requiring electronic disclosure; and
- 2) (keenly related to #1) In the U.K., unlike the U.S., the general rule is that the loser pays the winner’s costs, including attorney’s fees. This does a lot to discourage frivolous litigation. Mind you, after the case is over, the winner’s costs may be (and often are) challenged as being disproportionate. This results in an assessment of the costs, during which the invoices get nitpicked to death or the parties reach a settlement that both can live with. Otherwise, their argument is brought before a “Costs Judge,” which constitutes a roll of the dice.

In light of the above, computer forensics and electronic discovery have become huge business in the U.S., significantly less so in the U. K., where Laurie Watt observes, “We’re out of the infancy stage, but probably more in the toddler stage.” He expects that to change over time, as the U.K. surrenders its adherence to paper. For the moment, most discovery at Charles Russell (one of the top 50 firms in London and very well regarded) is still paper, and indeed, most of the evidence presented in court is in paper form. Only the very largest cases tend to be presented electronically, even when all the data gathering and review have been done electronically. Watt also notes that attitudes will change as younger, tech savvy judges come on the bench with an expectation of dealing with evidence electronically. But for the moment, clients are resisting even simple steps like converting paper documents to searchable PDFs, simply because of the expense, even though this process would allow electronic and paper data to be reviewed together.

Ian Henderson agrees completely, saying that his country has been slow in adapting to harvesting evidence from computers, and that he sees it done in less than 5% of cases. Henderson, who runs a very small but well known computer forensics firm, goes back long enough that he remembers “cutting my teeth on Norton Disk Editor as my first forensic tool.” On Henderson’s wall is a beautiful computer-generated time line for a case, which his client agreed to use in trial preparation but firmly declined to use in court. The client’s dismissive comment was simple: “The judge doesn’t like technology.” In this manner is great wall art born.

Henderson describes British litigation as “less argumentative than the U.S., rather more gentlemanly.” Even expert challenges, he reports, are fairly rare. If the expert has a reasonable CV and has previously qualified as an expert, he says there is almost no chance of a challenge. Most of the other interviewees tended to agree, with the notable exception of Watt, who good-naturedly told us how many experts he sees who are not experts at all and whose “bonkers” testimony needs to be “shredded and discredited.”

The general level of lawyer knowledge about electronic evidence was universally regarded as lower than the U.S., though lawyers are taking more classes to come up to speed – 16 hours of continuing legal education are required each year, and the number of EDD courses are proliferating.

Everyone seemed to agree that a lot of U.S. firms got burned when, as Henderson puts it, “they parachuted into the U.K. charging premium prices, only to find there just wasn’t the market that they had imagined.” Adrian Palmer said that many American firms dreamt of “a golden isle” which simply didn’t materialize. As he put it, “corporate counsel in Britain have much less of an appetite to spend money on electronic disclosure, unlike their American counterparts.” Some of the EDD invaders folded their tents and disappeared, other remained but with more modest staffing.

What is the major difference in electronic discovery in the U.S. and the U.K.?

There was no hesitation when asked to define the major difference between electronic discovery in the U.K. and the U.S. Everyone agreed that “electronic disclosure” (as it is

known in the U.K.) is principles based, whereas electronic discovery in the United States is rules based. To a man (yes, this seems to be primarily a male domain across the pond), our English friends like the principles based system better. Frankly, after listening to them, so do we.

In the U.K., attorneys must certify to the court that they have fully disclosed relevant information to the court. If their certifications are later proven false, they can be “stricken off the roll of solicitors” – in our terms, disbarred. As a result, attorneys are well motivated (ethically and practically) to sternly admonish clients that there will be no “hide the ball” tactics. In this country, we tend to administer sanctions, but we have only to read the headlines to realize that there is very little fear of disbarment. In fact, attorneys seem to be pushing the envelope when it comes to playing fast and loose with e-evidence here. It is no wonder that we’ve experienced such a rash of U.S. opinions in the last year and a half granting sanctions.

John Sykes says simply “If a client suggests that a particular document not come to light, I make it clear that it must be produced. No exceptions.” As he points out, knowing how seriously solicitors take their disclosure responsibilities means that clients don’t do a lot of shopping for solicitors based on whether they think they can control what is to be disclosed..

Aside from the rules-based vs. principles-based approach to EDD, is there another major difference?

Unanimously, the answer was affirmative. A staggering difference between EDD here and across the pond is the differing perspective on privacy. The European Union Data Privacy Directive, passed in 1995, required member nations to enact laws upholding the Directive. You might think all the laws would look pretty similar since they were based on the same Directive, but you’d be wrong. In the U.K., the rules are interpreted liberally to allow disclosure, especially of employee communications in workplace environments. The British courts, according to Henderson, are focused on “the fair disposition of justice – they want to know if the data is relevant – if so, it comes in.” Palmer notes that you must be sure that, as you are balancing the privacy rights against the employer’s interest, that there is a very legitimate business interest in disclosure. There is a fairly careful examination of the facts in each case to make sure that the possible intrusion on privacy is justified, though the actual bar to getting there seems fairly low.

Though examination of workplace activity is standard in the U.S., and liberally allowed in the U.K. where a legitimate interest of the company is involved and particularly where there is a “no privacy on company computers” policy, the Continent is far more strict. In many countries, an employee’s e-mail on a company computer is private. Period, end of quote. Many hurdles must be surmounted before that e-mail can be examined for use in a case. France requires individual consent, Belgium requires that data be processed locally, etc. As Darren Pauling noted, some U.S. companies have discovered to their chagrin that “Captain American can’t just go into Europe and grab data.” Many American firms have been burned by their ignorance of European privacy laws.

An interesting wrinkle exists in the U.K. If there is sufficient evidence to believe that a home computer may have been used for business purposes, Palmer says you can get to the computer pretty darn quickly – this seems to be more of a sticking point with American judges who tend to more closely guard privacy at home. In fact, British laws allow for the granting of an ex parte order which allows a forensic examiner, accompanied by a solicitor, to go unannounced to a home to image a computer on the spot, and sometimes to remove it for imaging. Palmer says the same procedure can be applied at the workplace as well. This is certainly a civil process that we don't have in the States.

Interesting question: will the U.K. allow shipment of data to the U.S. for a case? Our experts say yes, but it must be in response to ongoing litigation. Moreover, entire images are not shipped, rather the responsive, reviewed-for-privilege data is transmitted.

One judgment the authors formed during the course of all these interviews was that American law firms would be well served (unless they have a presence and their own contacts on the Continent) to work through U.K. firms, where everyone “sort of” speaks the same language. All of the English firms, even the small ones, are well connected on the Continent and can provide valuable gateway services to U.S. firms. They've seen all the problems, they know the ropes and they can explain it all to the Americans in English. Finding a trusted U.K. partner to advise U.S. counsel in these issues seemed a very good idea to us, and our interviews suggested that this is being done on a regular basis. It is not at all unusual, according to Henderson, for firms to find that as much as 50% of their work involves the Continent. Rahoul Bansali and Darren Pauling from KPMG agree, telling us that “the U.K. is the gateway into the Continent for many American firms.” All of computer forensics firms said that they had been regularly involved in American “beauty parades” competing for business. This is unlike computer forensics in the U.S., where only the largest firms currently tend to have significant work abroad.

Are there other striking differences?

Yes – according to Henderson, it is fairly common for two parties to have one expert, whether by agreement or because a single expert was appointed by the court. Special masters are a different matter. Though fairly common in the U.S., Sykes has very rarely seen the appointment of special masters to deal with e-evidence issues.

There are also probably more encrypted machines in the U.K., so standard practice is to image once and then image again after decryption.

And ESI – well, that's still largely an American term. It is generally electronic evidence or electronic data in the U.K.

Another difference, highlighted by Sykes, is that the attorney-client privilege can be maintained on workplace computers, whereas U.S. courts have frequently pierced the privilege, particularly where there is a policy in place that says that no activity on the employer's network is private and that the employer may monitor all such activity.

Bhansali and Pauling note that they don't have the sort of traditional litigation hold that the U.S. does – generally the preservation duty in the U.K. is triggered by a preservation letter. Unlike the U.S., there is no litigation hold where litigation or regulatory action is “reasonably anticipated.” Also, though there is less litigation, there is a great deal of regulatory activity – many more cases stem from that than litigation. They also point out that most British firms are “one-stop shops” – computer forensics and the management of electronic data are combined, whereas they see many more “processing shops” in America.

The emphasis on records managements, which looms large in the U.S. these days, is only slowly making headway in the U.K. The concept of being “litigation ready” is just gathering steam, so records management is probably not far behind. It has begun to occur to British companies that perhaps it is foolish to hold on to everything, but they are not yet taking out the trash with the speed of their American counterparts. Bhansali says he is just beginning to hear clients ask themselves, “What do we need to keep and why do we need to keep it?”

Family law? Apparently, it depends on who you talk to. Most of our computer forensics interviewees said there was very little ~~Nope~~ – though we see a lot of it in the U.S., our interviewees all looked startled at the notion. Using electronic evidence in divorce cases seemed to strike everyone ~~them~~ as “not the sort of thing one would ordinarily do.” However, Watt (whose law firm has one of the largest family law practices in the U.K.) was adamant that they see a good bit of electronic evidence, which made us think that it is considerably more prevalent in cases where there are substantial assets. It may well be that electronic evidence is used in the U.S. in divorce cases where the assets are far more modest. One striking comment about family law cases in the U.K. came from Grant Russell, a partner in Charles Russell who was kind enough to write us after our very reluctant return from the U.K. He mentioned that attorneys, private investigators and computer forensics technologists have all found themselves as defendants in his country for violating the privacy rights of spouses whose data has been accessed without proper authority.

Equally curiously, there didn't seem to be ~~We didn't find~~ a lot of interest in cell phone evidence, even in family law cases ~~either~~, in spite of the huge increase in the number of cell phones the American experts are seeing.

There is also very little spoliation, a point upon which all of our interviewees agreed. More common is the failure by companies to conduct a comprehensive search for relevant materials, though there was some disagreement as to how often this occurs. Henderson believes that businesses often do the minimum they can get away with, often not searching phones or peripherals for data. Not all of this is necessarily a consequence of bad intent - in fact, much of it is driven by cost concerns or a lack of records management. It is also true that, nationwide, many attorneys aren't particularly skilled in electronic evidence, and they sometimes fail to ask the probing questions necessary to uncover evidence. Henderson says it is “fairly common not to examine individual machines unless the need to do so sticks out like a sore thumb.”

What's the same in the two countries?

Computer forensic technologists in both countries bemoan that they are often called in at the last moment, that everything is an emergency and that lawyers are naïve about how long computer forensics can take.

Our “meet and confer” has an English counterpart known as the Case Management Conference. Here, the solicitors will come up with an electronic disclosure protocol, and agree on search terms, format of production and the timetable. Palmer notes that opponents are likely to consider full e-disclosure, very little e-disclosure, and a middle ground, finally settling on what makes most sense economically in light of the issues in the case and the amount in controversy. He says there is more agreement than disagreement in these meetings, so this is a distinct point of departure from their American cousins. It is the same sort of meeting, but it is far more likely to turn into a verbal brawl in the States, with many more hearings on electronic evidence disputes.

We've noted a recent trend in the U.S. to bring computer forensics in-house, at least to some extent. Palmer reports the same trend, largely in an attempt to conserve costs.

So what the heck is “proportionality?”

Proportionality is a big deal in the U.K. Essentially, as applied to electronic disclosure, it means that the level of effort that will be required by the court will be proportionate to the amount in controversy or perhaps the public importance of the issue being litigated. U.S. courts actually try to achieve the same thing, albeit not with that name. The English courts also use a similar line of reasoning to try to level the playing field for David and Goliath.

What kind of cases are the folks in the U.K. seeing?

To no one's surprise, commercial litigation leads the way, with an antitrust and the theft of confidential information cases close behind. There are many, many cases related to compliance issues. After, that employment law and civil fraud seemed to be the biggest sources of cases. There is a good bit of criminal work, but just as in the U.S., there are computer forensics firms that will accept the work and firms that do not. There ~~was, as are~~ some divorce cases, as mentioned previously, ~~a curious absence of divorce cases which is unusual to us though somewhat less than because small firms~~ in the U.S. where small firms often report that as much as 25% of their cases involve divorce.

How do they get their work?

Not much difference there – repeat business and referrals represent the majority of new cases. Many report getting business from conference appearances and articles, and, unsurprisingly, brand identification can be a huge factor, as indeed it is for KPMG, which was voted “Employer of the Year” in London last year.

Perhaps a bit different than the U.S., our British colleagues seem to have an especially keen focus on personal relationships, often cemented over an ale and fish and chips at a local pub. The authors noted that businesses lunches in the U.K., unlike most of those in the U.S., almost invariably involve alcohol. The colonies seem to have discarded a revered ancestral tradition.

What are the primary tools used for computer forensics and EDD in the U.K.?

The primary tools for forensic analysis? No surprise there. Just as in the States, EnCase and FTK are the two primary tools, supplemented by the usual jumble of software (off the shelf and custom) making up a forensic technologist's toolkit. For management and review of the data, Summation, Concordance and Ringtail were most frequently mentioned, just as in the U.S. All of the forensics technologists regarded themselves as vendor independent. Bhansali said emphatically, "We simply chose the right tool for the right job."

Most computer forensic firms seem to be using primarily search terms rather than utilizing conceptual search, which is regarded as more complex and expensive, and therefore relegated to only the largest cases.

What format is data being produced in?

This proved to be a funny question, because no one agrees in the U.K. any more than they do in the States. Some say paper, some save native, and some say TIFF with load files, others searchable PDF. So there clearly exists the same uniformity of opinion (not) that exists here – although we certainly do less paper production than our British relations.

What are the English charging for computer forensics and EDD?

Costs, as always, vary. However, the usual range among those we spoke with spanned from \$400-\$500 an hour, considerably higher than U.S. firms. (Note to one another: explore opening Sensei office in London). The average data theft case, as an example might cost \$10,000-\$20,000 when all is said and done. Retainers varied between \$1,000-\$10,000 depending on the size of the case. The bottom line bill for major cases seemed a bit of a delicate subject, as indeed it is in our country. Clearly, there are atmospheric invoices generated on both sides of the Atlantic.

These high costs are not well received by many clients, who seem to regard computer forensics as "IT work," and do not understand the science of computer forensics or its complexity and painstaking attention to detail. In the EDD arena, there as here, some companies insist on charging by a per page (using paper equivalencies for data) or per GB rate, which Henderson and Palmer both call "crazy," as it bears no relation to the actual labor involved. Palmer noted that the U.K., like the U.S., has a problem with less than honorable companies inflating their hours and tendering huge bills to clients. Often, he said, unscrupulous vendors will end up charging twice as much as the major EDD players, who nominally have a higher per hour rate.

Just as in the U.S., it is difficult to explain to clients that you cannot give an upfront estimate that makes any sense. Pauling remarked, “Transparency is a big part of what we done – but we need to see the amount of responsive data before we can give a sensible quote and we make that clear to clients.”

Lawyers aren’t cheap either. In what Henderson calls the “Magic Circle firms,” lawyers charge 600 pounds (roughly \$1200) per hour, thereby pricing themselves out of everything but the big-case, usually commercial, marketplace. As a consequence, Henderson sees a great reliance on in-house counsel and a tendency to shop around, often using different law firms for different purposes.

How are the English trying to save money on EDD costs?

Some clients are becoming “clued up,” which seems to be British speak for clients who are taking a lot of the EDD review in house and producing the relevant data to the lawyers for review. This phenomenon is still in its early days, but our experts expect it to become at least a minor trend.

Pauling noted that charges seem to be more commodity based these days, with fixed charges for imaging computers and flat fees based on volume of data, etc. We have seen the same kind of pricing in the U.S., though it is arguable (on both sides of the ocean) whether monies are genuinely saved overall.

Sometimes, parties agree to use a single expert, which hardly ever happens in the States. This seems to be part of the more agreeable nature of British litigation, as well as a concerted effort to save on costs. In other cases, the court may appoint a single expert.

What costs are causing the most angst?

Certainly the lawyer cost associated with reviewing the data is a problem, there as it is here. Ditto for the high cost of hosting case data online, \$4000 a month for a single case being fairly common.

What kind of security are computer forensics firms using in the U.K.?

The smaller firms might rely primarily on locked doors and biometrics on lab equipment, but most of the U.K. has exterior cameras everywhere, and there are often uniformed guards at commercial establishments. Fireproof safes are standard. In the larger firms, such as KPMG, the security is more intense, with badges issued, visitors escorted (thank you Rahoul, for ceasing your escort at the door of the ladies room!), and individual carded entry into particular rooms or floors.

So who is doing computer forensics in the U.K.?

Many of the small (often solo) shops are run by former law enforcement officers, often with their primary experience in child pornography and no commercial experience. This

parallels the U.S., where these firms are quite common. The big companies are there – KPMG, Kroll Ontrack, Deloitte Touche, PWC, Ernst & Young, and others. KPMG has a 100 plus computer forensics department, with approximately 70 people in the U.K. and the rest on the Continent. There are a number of smaller private companies, like Palmer Legal Technologies and Advanced Forensics, who cheerfully fly beneath the radar of the “whales.” As Palmer noted happily with a classic British proverb, “The proof of the pudding is in the eating.” Frequently the major companies need to reel in some assistance quickly, so sub-contracting is a big business segment for the smaller firms. Much as we see in the U.S., smaller firms are, as Palmer terms it, “hoovered up” by the large concerns. He has not, however, seen a lot of firms “belly up,” which is in striking contrast to the U.S. where the competition for business has resulted in a lot of marketplace shakeout.

Training varies widely. As you might expect, KPMG has rigorous training, involving a minimum of two weeks of training in EnCase, FTK boot camp training, and six months of in-house training, culminated by a “sign-off” from the employee’s supervisor that the training has been satisfactorily completed. There is training on individual software as well, some done by vendors and some in-house.

There is no regulation by the government, as indeed there is no regulation by the federal government in the U.S. Most examiners, however, will follow the U.K. ACPO (Association of Chief Police Offices) best practices guidelines.

What does the future hold for U.K. forensics?

Forensic computing may never be the formidable presence in the U.K. that it is in the U.S., but we learned a little about the future from interviewing Ian Mitchell and Carlisle George, both Senior Lecturers in forensic computing at Middlesex University. This is “year one” of their program, so they are feeling their way a bit gingerly, but with a great deal of excitement as the demand for this curriculum grows. Currently, only a small handful of universities offer forensic computing training, so Mitchell and Carlisle are proud to be pioneering a new program.

They are currently in the process of setting up their lab, using FTK and EnCase as their primary tools, and Paraben for their cell phone forensics.

Carlisle is also a solicitor, so their students are getting a healthy injection of the law along with the forensic computing. Their group is small – just a couple of dozen students – but they are not lacking in enthusiasm. In fact, the “CSI effect” that we’ve seen in the U.S. seems to have replicated itself in the U.K. Their curriculum delves deeply into computer science – they want to make sure they are not producing “point and click” jockeys who can only ride the software and don’t understand anything under the covers.

From their point of view, there is a wave of forensic computing technologists just over the horizon, all of them keen to understand the science of their trade, and to refine the processes. Most of those practicing this profession now came from other fields, but the

future in the U.K. belongs to those who will begin their computer forensic education as an undergraduate, a possibility which never before existed. That same phenomenon, of course, has become a part of education in the U.S., where computer forensics is now a major at several universities.

Thanks to all of those who were so cordial in granting us interviews and sharing their expertise with us. Our U.K. adventure was, in the words of your country, “bloody brilliant.” We are most dreadfully sorry that we can’t nip off to the pub with you once again and ‘ave a pint!

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology and computer forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com