FRAUD LAWYERS ASSOCIATION LECTURE

6th April 2016

E DISCLOSURE - PRACTICAL LESSONS FROM R v R CASE

The Issue

Complex and Lengthy Criminal Trials – Justice Working Party – 3 March 2016

" Information provided by the Legal Aid Agency demonstrates that there has been an average of 26 CLT cases per year over the last nine years. Defence costs alone averaged £2m and length in 2014 averaged 1,400 days from the point of representation order (excluding the investigation stage)."

Complex and Lengthy Criminal Trials makes important recommendations for each stage of a case - investigation, pre-trial and trial - to reduce the disproportionate impact of CLTs upon our justice system and the parties involved.

In the Working Party's view, the singular cause of difficulties in modern CLTs (which we have defined as cases of 60 days trial length or more) is the need to deal with electronic material: reviewing vast amounts of seized digital material in multiple formats for relevance; identifying the evidence to form the prosecution case; considering whether material is disclosable; and presenting the material at trial. These are the procedures which result in undue length and complexity, and in unacceptable delay. They can lead average cases to become lengthy and complex, and make already complex cases unmanageable.

Building upon existing guidance and the recent Leveson Review of Efficiency in Criminal Proceedings, the solutions lie, we consider, within three broad themes across each stage of a trial:

- *First, early engagement of relevant expertise at the investigation stage to ensure that the seizure and search of material is focused and proportionate to the alleged criminal activity and of trial counsel at the pre-trial stage, to ensure that disclosure takes place as early as possible, and that the issues in the trial are identified.*

• *Second, case management, by senior and independent law enforcement and prosecution agencies at the investigation stage, to ensure that the investigation is focused and progresses as quickly as possible, and by the same trial judge from the start of the pre-trial stage through to the trial, who can assist the parties to narrow the issues and present a clear case for the jury to consider.*
• *Third, adoption of agile and intuitive technology, built by the criminal justice system to meet its investigation and preparation needs, without compatibility boundaries across police forces, prosecution units or defence firms, which enables all trials to be presented with visual aids rather than reams of paper.*

Historical Context

- Technological Innovations – email, mobile phones, android devices, proliferation of communications.

Prior to 1996 gradual evolution of technology from Electronic Typewriter/Faxes in the late seventies/early eighties. The advent if the internet and specifically email had a major influence on the volume of digital communications. WWW invented by Time Berners Lee in 1989.

In 2015, 78% of adults (39.3 million) in Great Britain used the internet every day or almost every day. This was more than double the proportion of adults (35%) that used the internet daily in 2006, when directly comparable records began. Daily internet use increased by 2 percentage points since 2014 .

In 2015, 74% of adults had used the internet "on the go" using a mobile phone, portable computer or handheld device (as shown in figure 3). Almost all adults aged 16 to 24 (96%) accessed the internet "on the go", compared with only 29% of those aged 65 years and over.

Of the internet activities surveyed in 2015, email remained the most common, with 76% of adults having used the internet for this purpose. This was an increase of just 1 percentage point since 2014, but 19 percentage points since the 2007 estimate of 57%

(Source Office of National Statistics)

In 1996 0.9% of the world's population (36 million) used the internet. By December 2015 it was 46.4% (3.36 billion). In 1996 16% of households in the UK had mobile phones. By 2014 it was 94%.

(source Statista 2016)

- The CPIA 1996 – tackling the "keys to the warehouse" phenomena. Defence lawyers spending a disproportionate amount of time trawling through a mountain of hard copy unused material. This created inordinate delay in the criminal process. Solution was a more structured and focused disclosure process. Two stages, Primary Disclosure-Defence statement – Secondary Disclosure. Looking for material that might support the defence case or undermine the prosecution case. It was a continuing duty throughout the proceedings.
- Protocols and Guidance re e disclosure -2011 AG Guidance of Digitally Stored Material.
- Problems – LPP, Third Party Disclosure, Software Options, Dip Sampling v Whole Dataset, Management of the Process by the Court including available sanctions for non-compliance.

1. ***R v R (2015)EWCA Crim 1941***

- Brief history of the case – the area of dispute, decision to stay and CA judgment

2. Some practical problems with e disclosure

Prosecution must lead the process (para 34)

Such an approach must extend to and include the overall disclosure strategy, selection of software tools, identifying and isolating material that is subject to legal professional privilege ("LPP") and proposing search terms to be applied.

- LPP – the removal of. How is this best achieved? Should the whole process be supervised by Independent Counsel? (Consider the recent SFO decision – *R v*

McKenzie **[2016] EWHC 102 (Admin)** - per LJ Burnett (QBD Admin) endorsing the SFO handbook procedure for the identification of LPP material in seized dataset by using their in-house software came up with the following guidance:

In my judgment, a seizing authority has a duty to devise and operate a system to isolate potential LPP material from bulk material lawfully in its possession, which can reasonably be expected to ensure that such material will not be read by members of the investigative team before it has been reviewed by an independent lawyer to establish whether privilege exists. That approach to LPP material imports the necessary rigour required by the law for its protection in this context.

There is a world of difference between determining whether something is protected by LPP, which involves close consideration of the content and context of a document or communication, and identifying a document, file or communication as potentially attracting LPP, which does not. As is plain from the description of the system for separating electronic files by the use of search terms there is in fact no need for the electronic file to be viewed at all.

Rejected the claimant's arguments that the SFO procedure breached the AG Guidelines on E Disclosure (2011) and/or was unlawful as defined by previous case law.

The broader problem is whether the software utilised by the investigator is actually fit for purpose. How effective is it in practice in removing LPP material from a dataset? Consider the problems created by lengthy email chains, the saving of attachments in different formats, duplicates. The more sophisticated the software the less likely this is to occur.

What about the removal of LPP or indeed any material by a third party in response to a production order? How reliable is such a process? How much involvement should there be by the prosecution? Is it really safe to leave this process to the third party especially where it may also be a prosecution witness. Isn't the reality that the sheer logistical demands of such an exercise are being delegated to the third party to save time and resources. With greater technological innovation might it not be better for the prosecution to take on this function? The idea that parking this issue with the third party to resolve is a time saving measure is a myth. In practice the prosecution tend to "park" the issue behind other aspects of case preparation. This often proves a false economy. Third parties will not be pro-active as its rarely in their interests to be so.

- Planning and Understanding the limits of software capabilities.

The prosecution need to plan the exercise like a military campaign. Consider prioritising certain computers of particular interest. Work towards time limits and resource accordingly. Should avoid playing catch up and "get it right the first time". Consider whether you need outside input from an IT contractor. A key question is whether the software that you use to interrogate the data and find evidence will be suitable to deliver proper e disclosure. The interrogation of data to identify evidence is not the same process as organising data and presenting it in a user friendly format. However, if you decide that you need to re-process the data in order to deliver a coherent package to the defence consider how data might be corrupted in that process.

The production of a Disclosure Management Document/Plan is now a far more routine procedure. It is imperative that it properly tackles e disclosure and specifically the issues outlined above.

- Co-operation between Defence and Prosecution – *"The prosecution must then encourage dialogue and prompt engagement with the defence"* (para 34)

Dip Sampling

This generally consists of agreeing search terms to be applied to the data to identify material that might undermine or assist. At this stage there will have been no defence statement. Thus the Crown are forced to make an educated guess unless the defence has been set out in interview or possibly a detailed prepared statement. In R v R at an early stage the defence were ordered to produce "issues documents" which would help to crystallize the issues to assist the process. Not sure there is any legal basis for this but it does make a certain amount of sense. And the CA would appear to discourage judges from making orders that "confuse or conflate the various stages of the process"

I think there is possibly scope for the judge to require the prosecution in appropriate cases to more accurately focus the issues by amending there case summary. I have been in cases where the trial judge has required the service of a shorter and more focused document

Most important to make a distinction between search terms which are designed to turn up evidence of the alleged offence and those designed to ID "unused material". There is a tendency amongst some prosecutors to merely tack on a few additional terms suggested by the defence to those already applied to the dataset. This to my mind is intellectually lazy and not a correct application of s3.

The idea that a large number of search terms will lead to a greater number of hits is actually incorrect. What needs to be avoided is the inclusion of too many simple words like "too" and "what". Focused terms will produce better results. Proportionality is not an unreasonable objective of the process can be described as properly forensic and within the defined parameters of the issues between the parties. Remember this is the first stage of the process. There will be scope to return to the dataset with additional search terms during secondary disclosure after DS have been served. Can also be the subject of a s8 application.

We should be wary of a dip sampling process that results in only a handful of documents being disclosed. 1% of 7 terrabytes of material is never going to be truly representative of "relevant" material especially where the case is being prosecuted in a broad and unfocused manner..

However, there are particular difficulties in re-constructing email chains by using the dip sampling method. Email chains may continue over several months. They can go off on weird and wonderful tangents with "Sub-conversations". The problem with isolating a single email is that you lose context. It is the main argument used to justify serving all email data on the defence so that it may be fully interrogated. It is resisted by the prosecution and the courts as being the keys to the warehouse by the back door. But is it really? Such is the sophistication of e discovery software now that the defence can themselves search this data "intelligently" and denude it to manageable and focused proportions. The LAA (if they fund) are not going to allow the defence teams unfettered access to all of this material. They will require a focused and proportionate approach to be adopted. This in effect passes the resourcing of the exercise over to the defence. Would it actually create further delay? Its arguable. Even where agreed search terms are applied a huge dataset can and frequently does result. If the prosecution are required to review it (or a sample of it) that creates its own delays and if it is not sufficiently rigorous can result in mistakes being made. Who knows better what to look for then the defendant? Requiring this logistically demanding task to be conducted by the prosecution can prove to be a false economy.

- **Management of the process by the court** – *The law is prescriptive of the result not the process*

Paras 39 et seq emphatically reject the notion advanced by the Attorney General's counsel that the judge should not play an active part in the management of initial disclosure for fear that it would be inconsistent with the statutory regime. This is entirely consistent with the more robust case

management regime that Leveson has championed in his reform of the criminal procedure rules. His mantra being to "get it right the first time".

However, it is not clear exactly how far the judge is allowed to go in intervening in this process. Taken at face value the CA seem to be saying that the judge should be pro-active in ensuring that the prosecution reach the stage where they "purport" to have provided primary disclosure as soon as practicable. The CA observe that "substantial compliance" with the s3 duty should be sufficient. It's not clear to me what "substantial" actually means in this context. The CA were wary of being too prescriptive. But what does amount to "substantial compliance"? Is it enough for the Crown to have scheduled up the material that they have reviewed and to have disclosed a mere handful of documents? How detailed should their descriptions of the content of the documents be? What is an acceptable dip sample in the circumstances? What if the judge does not deem that the prosecution have substantially complied with their duty? What sanctions are available to the court in such circumstances?

- Flexibility

The CA do not discourage the judge, after discussion with the parties, from devising *"a tailored or bespoke approach to disclosure. That must certainly be preferable to dealing with the matter in a mechanistic and unthinking way"* However, the scheme of the CPIA must be kept firmly in mind and the aim must be to make progress in accordance with the defined stages of that regime. They caution that if the CPIA regime is not kept in mind an apparently attractive short-cut may lead to the case (as in R v R) becoming bogged down in satellite litigation.

But what if the regime is followed and the prosecution for whatever reason fails to deliver disclosure in accordance with the scheme agreed with the defence and the court? Perhaps due to technical inadequacies on their side. How is the court to address that situation? Let us say for the sake of argument that after an initial dip sample the Crown purport to have given initial disclosure. Defence statements are served. These trigger a much wider trawl through the dataset and the disclosure of hundreds of thousands of pages of additional material. This process of review and disclosure takes literally months if not years to complete. How has the adherence to the statutory regime actually achieved any more efficient disclosure? If what one is left with is an incoherent mess. There will be plenty of s8 applications which will tie up the court and create further delay.

As an aside the CA observed that it is no part of the prosecution's obligation to improve on the format of the material to be served. There is a distinction to be drawn between improving on the

presentation and search-ability of material and improving on the material itself. The former merely involved re-organising it for the purpose of defence and prosecution review. The latter might result in it's alteration and compromise its forensic integrity.

That may be accepted but what if the only way in which to properly present one's defence involves the painstaking reconstruction of email conversations over a period of years? It may well be that the only effective way to do so is to have access to the whole dataset as imaged from all relevant devices. Should the defence be prevented from having access to all of that material and if appropriate the ability to re-process it to re-construct those conversations? If that is the case then surely it creates scope for unfairness.

Conclusions

1. This issue needs to be tackled head on because it is creating undue delay and increased costs. The fairness of the process is being compromised. Both prosecution and defence need to engage in a discussion as to how things might be improved.
2. We need to move away from the atmosphere of distrust that seems to permeate any dialogue between the prosecution and defence. The notion that prosecutors deliberately bury useful material in the unused or that defence lawyers manipulate the system to derail the process.. Neither position should be tolerated and there needs to be a consensus that achieving a fair and measured response to these problems is mutually beneficial.
3. There needs to be a dialogue about the most cutting edge software available and whether on a cost benefit analysis investment in the use of such software and (possibly) independent expertise will actually improve the efficiency of the process. There should be a drive to achieve best practice across all prosecuting agencies not just the SFO.
4. In appropriate cases the possibility of there being complete disclosure of all email traffic between named custodians should be contemplated where a case can be made for it. This will ensure fairness and also pass the burden of resourcing such a review to the defence which frankly is where it should be.
5. We should learn from the progress made in the civil sphere – Susan Monty.

Steve Sharp ssharp@bivonas.com
Bivonas Law LLP www.bivonaslaw.com
24 Cornhill
EC3V 3ND
0207337 2659 (direct dial)

LEGAL DISCLAIMER