ISSN 1758 8421

Criminal Law News

THOMSON REUTERS

Contents -

PUBLISHED BY SALLY RAMAGE
COPEHALE, COPPENHALL, STAFFORD,
UNITED KINGDOM

TEL 01785 - 211370
FAX 01785 - 228281

WWW.CRIMINAL-LAWYER.ORG.UK

An urgent need for mandatory rules on bio-information and digital database evidence in legal systems

Sally Ramage

Lack of mandatory rules on bio-information and digital Police database

The English justice system blissfully continues to pay scant regard to the lack of any mandatory rules as regards bio-information and digital police databases. There are gaping holes in the English legal evidential system. These holes allow cross-country bio-information evidence, gathered in non-mandatory ways in other countries. Our own police databases of digital and bio-informaton, (as confirmed by 'auspicious' bodies such as the Parliamentary Select Committee in 2005), derogating our citizens' data protection and human rights, sanctioned by parliament and in common law precedents, are themselves evidence of the total inertia to the acute problem of digital and bio-information evidence in English courts, much of which goes unchallenged and unquestioned. This paper seeks to highlight these problems in the hope that action will be taken.

Courts accept anything with a scientific name

The courts have failed to perceive the gap between *optimistic theory* and *hard proof* and they have accepted weak forms of validation with regard to fingerprints, DNA evidence and other bio-information. There are no mandatory rules concerning the analysis of forensic evidence. Looking to *Pepper v Hart*[1], one can see its unauthorised extension by English judges to quote from any legal article, report, or written material. The 'free-for-all' extends throughout the English legal system, remaining biased, even though

attempts to codify the law in the Criminal Justice Act 2003 are strongly resisted and very slowly enforced, some would argue[2].

Nuffield Report: "The forensic use of bio-information: ethical issues"

The Nuffield Council on Bioethics, subsequent to its consultation carried out on behalf of the Home Office, produced a report in 2007 titled "The forensic use of bio-information: ethical issues", in which bio-information is described in paragraph 1.9 as

"…derived from the analysis of a range of physical or biological characteristics of a person. It is most often used in efforts to identify individuals or at least to differentiate individuals from each other..."

At paragraph 1.11. the report states that:

"…retrieved 'trace information' can also support inferences about what a person did when they were at a scene of a crime, such as handle a weapon, or have sexual intercourse...".

This report followed the 2005 Seventh Report of the Select Committee on Science and Technology, which had concluded that the English legal system needs specialist judges and lawyers for cases relying on complex forensic evidence. The report concluded,

"There are certain areas, such as the digital evidence specialities, which are becoming critical in a growing number of cases. Furthermore, the potential complexity of such cases is escalating all the time. A spin off benefit to offering specialised training to lawyers would be an overall increase in the number of scientifically literate lawyers (and thus, in the fullness of time, judges). We recommend that the Home Office issue a consultation on the development of a cadre of lawyers and judges with specialist understanding of

specific areas of forensic evidence. An additional benefit to this would be the creation of a small group of judges and prosecution and defence lawyers with the ability and current knowledge to act as mentors to their peers when required."

Digital databases

Be aware of electronic footprints, because if something is deleted from a computer it might still leave evidence in the metadata, the theory goes. Metadata can assist in proving the authenticity of the content of electronic documents, as well as establish the context of the content. Metadata can also identify and exploit the structural relationships that exist between and within electronic documents, such as versions and drafts. Metadata allows organizations to track the many layers of rights and reproduction information that exist for records and their multiple versions. Metadata may also document other legal or security requirements that have been imposed on records; for example, privacy concerns, privileged communications or work product, or proprietary interests.

Is this true? No.

As an example, Microsoft 'Excel' spreadsheets can be wiped clean and the metadata prior to production can be removed. Excel spreadsheets are different to other file types in that when they are converted to an imaged format, the formulas used to create the spreadsheets, the metadata, cannot be reviewed without looking at the original file. The formulae used to calculate the values displayed in the cells is the metadata and is integral to resulting spreadsheet numbers. However, file names, dates, and authors may be deleted, along with recipients, printout dates, changes and modification dates, and other information.[3]

Challengeable bio-information

Cells and data can be locked, making access impossible. This has enormous implications for electronic document production in court. In sum, metadata can be altered intentionally or inadvertently, extracted during native file conversion, and may be inaccurate!

Therefore, most of metadata has no evidentiary value, and any time (and money) spent reviewing it is a waste of resources. Therefore, electronic evidence is poor evidence and must be challenged.

In the UK, specialist police established for the gathering, creation and circulation of criminal intelligence are faced with some difficult organizational problems of "digital divide, noise intelligence overload, and intelligence gaps"[4].

The UK intelligence overload is due to noise and a lack of analytical capacity and administrative support. In some circumstances, out-of-date information clutters up the information environment, and takes up valuable time, besides which, data must be periodically purged in keeping with data protection guidelines[5].

Intelligence-led policing systems need more and more data and this is more data than the police can cope with. For instance, suspicious transactions reports (STR's) during the times they were relevant[6]. However, this does not mean that the intelligence system is better since no analysis of the data had been produced. Therefore, no one knows if it is bad thing or a good thing. This may be one reason why the UK 2007 Money laundering regulations were drafted with an onus on professionals- to decrease the amount of low-grade reports, never analysed anyway.

The police databases contain reports derived from intercepts, covert and overt

The system in place is highly organised. However, the content of such data is as behoves each person inputs into the system .This, therefore, is the flaw. The flaw is not in the process[7] but in the unregulated ad-hoc content of a report written by a non-lawyer, being included at will into a national digital database, transferrable inter-country at will even though there are probably millions of errors, duplicates and incorrect pieces of information in these databases, when, once merged with transatlantic and other systems' database becomes a useless soup of incoherent information. For data must be processed in small pieces for any errors to be flagged up and for careful duplication to be removed.

Since people's liberty is at stake, it is of utmost priority that out security, defence and criminal data be carefully protected and guarded and altered only by qualified vetted personnel. Qualifications are of utmost importance. There will be criminals who will stop at nothing to obtain a country's data free of charge in order to sell it to pharmaceuticals; subdivide it into areas of financial value; manipulate it to sell bespoke to other governments; or alter it to affect certain persons irrevocably. Data is power. Data is intelligence. Data predicts. Data can be manipulated to weaken our defence against terrorism. Data is more valuable than money or gold.

Digital confusion

An example of digital divide occurs when in one UK police force data pertaining to handguns, firearms and ammunition is stored on two separate and antiquated desktop computers, the two databanks created at different times and

for different purposes, with each system storing slightly different information and neither complete on its own.

This digital divide can cause particular problems in self-regulated cross-border or inter-institutional information flow.

Bio-information as evidence, the Borders Act 2007 and "eye prints"

The UK Borders Act 2007[8] enables a compulsory identity card for non-EU nationals and this will require immigrants to submit a biometric document that includes "features of the iris", effectively giving rise to an 'eye print' database. Iris recognition has been on trial in UK airports since 2005 but this trial reported that iris-scanning technology is not up to the standard required to sustain the ID card scheme. The UK National ID card system will nevertheless become a police super database from which UK police will be able to compare bio-information from the ID card database.[9]

United States: "Iris recognition" is a genetic privacy matter

In the United States (a country whose lead the UK Home Office usually takes), the use of iris recognition is treated as genetic privacy and a U.S. Genetic Information Non-Discrimination Act 2007 was introduced to protect people in the United States from being denied jobs or insurance. The US Genetic Information Non-Discrimination Act is the first US federal law to prevent employers from collecting genetic information on their employees and prevent insurers from denying coverage or from charging higher premiums based on a person's predisposition to disease.[10]

The US Genetic Information Non-Discrimination Act 2007 was passed after twelve years of its debate. This is as it should be, and a recent federal justice

department survey of American federal forensic laboratory procedures raised much alarm.[11]

Identification using scientific methods

The analysis of fingerprints, tyre tracks and bite marks are not as reliable evidence as researchers once believed, and crime-scene specialists told the National Academy of Experts.[12] Such bio-information is used in DNA sampling and fingerprinting. Iris recognition, fingerprint matches,[13] and facial matches all come under the issue of identification.

Fingerprint use and the law

Since 2001, the processing of fingerprinting has been automated in the UK, using a product named LIVESCAN and police in the UK hold 6.5 million sets of fingerprints as well as 1.2 million crime scene fingerprints in the "Unidentified Marks Collection".

In the UK, the Police and Criminal Evidence Act (PACE) 1984 and principally, Code D of the Codes of Practice regulate the area of identification for criminal purposes. The rules for identification differ between those cases where the suspect is 'known' and those where the suspect is 'not known' and PACE Code D, paragraph 3.4 defines the term 'known' as where 'there is sufficient information known to the police to justify the arrest of a particular person for suspected involvement in the offence'. PACE Code D (paragraph 3.1) requires that a first description provided of a person suspected of a crime (regardless of the time it was given) must be recorded. Samples are taken from those arrested as well as victims regardless of age or non-criminal background and this raises a number of legal issues concerning the interpretation, retention and profiling of bio-information. Section 78 of PACE gives the courts a discretion to exclude

from criminal trial evidence, which has been obtained unfairly. The three main factors which recur in the decisions under s 78, are 'bad faith' on the part of the police; impropriety in the form of breaches of PACE or its Codes of Practice and the effect of such impropriety on the outcome of the case[14] the legislation that governs bio-information gathering is the Criminal Justice Act 2003, which permits police to take fingerprints and biological samples from any individual arrested for a *recordable offence*, without their consent, whether or not DNA or fingerprints are relevant to the crime being investigated. In Northern Ireland, such bio-information is sent to the UK database where it can be kept indefinitely. In Scotland, such bio-information is retained for only three years, with extra two-year retention if an application to retain is made by a police chief constable. The Criminal Justice Act 2003 gives *exemption* to the police from the Human Tissue Act 2004, which makes it an offence to have any bodily material to analyse the DNA in it without consent. Though there are many cases of fingerprint errors, the police and police forensic officers are immune from prosecution[15], although this is unfair and against the doctrine of 'equality of arms'.

Facial recognition other than by comparison with a database

In the United Kingdom, fingerprint evidence has proven unreliable in a number of high-profile 'miscarriage of justice' cases. In ***R (on the application of Howe), v South Durham Magistrates' Court*** [16] the claimant was charged with driving whilst disqualified and without insurance. He did not admit that he was the Christopher Howe who had been disqualified[17]. The prosecution wanted to prove that the defendant standing there before the court was the person disqualified from driving. The prosecution applied for a witness summons to be

issued to a solicitor acting for the Christopher Howe who was disqualified. This solicitor was acting for the claimant in respect of the present charge. The claimant's representatives argued that this would be a breach of legal professional privilege and a breach to the claimant's right to a fair trial as per Article 6 European Convention on Human Rights, a breach of his right to choose[18] the solicitor to represent him and a breach of his right not to incriminate himself.

A criminal charge depends on the application of the three criteria described by the Court of Human Rights in *Engle v Netherlands*. These criteria are-

(i) the categorization of the allegation in domestic law;

(ii) the nature of the offence and

(iii) the severity of the penalty attached to it.

Article 6 contains implied rights of access to the courts, right to be present at an adversarial hearing, right to equality of arms, right to fair presentation of the evidence, right to cross-examine and right to a reasoned judgment.

Facial recognition database

Merseyside police uses facial recognition technology to take images of prisoners, which are stored on a national database. The software they use is Affinity automatic facial recognition software, which is manufactured by a company named Omni perception Ltd. Northern Ireland police use CCTV facial recognition technology called ABM's Facial Verification Bureau (FVB). The FBV turns images into forensic evidence for court submission by analysing facial and other visual evidence. It then compiles identification reports and provides expert testimony for use in a case. The automated facial recognition software is a powerful tool for the police used to search faces obtained from CCTV footage. It is used for immigration purposes in the UK.

Research findings on computer-based identification systems

Studies have shown that computer-based line-ups would be better than the physical line-ups, yet this method is not being used. As to the use of CCTV, research findings are not promising. Henderson, Bruce and Burton (2001) filmed, on poor quality CCTV cameras, typical of those used in high street banks, a mock bank raid where two robbers were involved.

The best still image of each robber was edited from the footage and one hundred participants were shown these colour images in conjunction with two TPO photo arrays (one per robber) of eight similar looking people and then asked to identify each of the two robbers.

The task was done poorly with a low hit-rate and there were many selections of the wrong individual. Using better quality equipment, the mock event was filmed again, but this time one robber wore a hat to conceal their external facial features, and the second 'robber' did not.

In a similar research paradigm, participants were also asked to identify the robbers. It was found that the robber without a hat was identified with a 64% accuracy rate but this dropped considerably when the target wore a hat. Learning a face takes time and repeated exposure under different viewing conditions (Bruce et al, 2003).

Ear-print evidence

In a case brought perhaps to test whether the court would now accept ear-prints as evidence, it was held that ear-prints were not sufficient and not tested evidence. The case of *R v Mark Kempster*[19] was a prosecution for burglary in which the detail of ear structure provided an inexact match. Kempster (K) had been arrested on suspicion of the burglary of an elderly woman's residence. The

police had recovered an ear print from the windowpane to the side of the window that had been forced in order to gain entry to the property. K was convicted and sentenced to ten years' imprisonment. His appeal was dismissed. K referred the matter to the Criminal Cases Review Commission. His appeal was then allowed because, although a comparison of the print on the windowpane with that taken from K was similar in shape and size, it did not provide a precise match. The earmark could not be relied on by itself as justifying a guilty verdict.

This is a similar case to ***Chief Constable of Avon & Somerset v Jest***[20], when the defendant's left thumbprint on internal rear view mirror of a car was held to be insufficient evidence of possession to found a charge of taking without consent. Of course, UK police fingerprint databases have been found to be compatible with citizens' human rights as per ***R v (1) Chief Constable of South Yorkshire police, ex parte LS (by his mother & litigation friend JB); R v (1) Chief Constable of South Yorkshire police, ex parte Marker***[21]**.**

In other words, a blanket policy of retention and use by the police of DNA samples and fingerprint evidence, after a suspect had been cleared of the offence that gave rise to the collection of such evidence, was deemed compatible with the Human Rights Act 1998

Other Jurisdictions' databases of fingerprints and other bio-information

Whether fingerprint evidence from other jurisdictions' databases are allowed in English cases is an issue which was flagged when the prosecution sought convictions by adducing copy certificates of judgments from Holland's police fingerprint records in ***R v Mauricio*** [2002] EWCA Crim 676. The defendant submitted that proof by fingerprint evidence under s.39 Criminal Evidence Act 1948 did not apply where the conviction was a foreign conviction. This is a

fact. The defendant relied on ***R v Nye***[22], a case decision that said that the best course where spent convictions[23] were in issue was to get the judge's ruling at the outset of the case. Nevertheless, the evidence of the 16-year-old conviction of the defendant was admitted. The defendant appealed against this decision. Mauricio's grounds of appeal were that the judge should have made a ruling at the beginning of the case as to whether the defendant was entitled to be treated as a man of good character and that a foreign conviction could not be proved by fingerprint evidence[24]. This appeal was dismissed on the irrational ground that it was not for the judge to declare whether the Crown was able to prove or had proved its case, taking the argument out of context.

In the case of ***R v Dumpster***[25] the decision was that it was for the defendant, not the court, to decide how to run his own defence. It is for the defendant to decide whether he was going to put himself forward as a man of good character. The prosecution in ***R v Mauricia,*** by using section 3(7) Criminal Justice (International Cooperation) Act 1990, obtained documentary evidence and not bio-information evidence from a foreign prosecuting authority. Furthermore, that foreign documentary evidence easily be used later in a civil proceeding[26], breaching UK employment laws. Dismissing this appeal case also runs against the grain of the rules relating to sexual abuse disclosures of minors[27]

UK Footwear database

Police have footwear databases. Footprints are the third most common type of forensic evidence after blood and DNA. The Forensic Science Service have an online footwear coding and detection management system using Footwear Intelligence Technology (FIT) which is updated daily and contains thousands of footwear patterns including sole and upper shoe images, brand logos and

examples of each type of footwear. One software programme called Solemate, contains more than 12,500 sports, work, and casual shoes. Its purpose is to identify shoes from shoe prints recovered from scenes of crime. Each record of this software contains the shoe manufacturer, the manufacturer's reference for that shoe, the date of that shoe's release on to the market, an image, or offset print of the sole, several pictorial images of the uppers and a set of pattern feature codes that facilitate search and match operations. Where different manufacturers have used the same sole unit, Solemate records are linked to allow the operator to consider all the footwear that might have been responsible for a crime scene print.

To use the database, the pattern of the unidentified shoe print is first assigned a set of codes, a simple procedure that requires the operator of the software to identify elemental pattern features within the shoe print, such as circles, diamonds, zigzags, curves, blocks, etc. The Operator selects from those options that best match the features within the shoe print.

The codes assigned to these pattern features form the basis of the database search. The results of a search are presented in descending order of pattern correlation.

National Integrated Ballistic Information Network

It will not be long before a handgun database is set up in the United Kingdom. The number of illegal handguns in the United Kingdom is unknown. The handgun database situation is much more developed in the United States where it is legal to own a handgun.

The US federal government keeps a ballistics database called the National Integrated Ballistic Information Network, which collects information on guns used in crimes.

This federal database has been credited with nearly 25,000 interrogations, many of which yielded investigative information. Researchers have found that imaging is helpful for generating leads but that the current technology for comparing tool marks is limited.

The United States federal database of all guns is similar to the UK database of shoeprints. In the United States, databases of handgun "fingerprints" are kept, but to date, such databases in various states have not been used in a criminal prosecution[28]. There is also a United States ballistics database, but this is not linked to any of the states' databases of handguns. Like the United Kingdom shoeprint database, the handgun database of New York, known as the New York Combined Ballistic Identification System and holds information about more than 200,000 new pistols and revolvers sold in New York.

Unique shell casings markings

New guns are test fired, and the minute markings the guns make on the shell casings are recorded and entered into the digital database. These markings are said to be as unique as fingerprints and can be compared against shell casings found at crime scenes. There are now 209,239 casings entered into New York's database. If there is a criminal offence committed with the use of a handgun, the shell casings can be interrogated with the database to ascertain the type of gun used, even though a file-down bullet, in a similar fashion to filing away a vehicle's chassis number (VIN), will defeat the database. The fundamental assumption that every gun leaves a unique mark has not been s[i]cientifically demonstrated, although a new method of 'micro-stamping'- a new technique used by some manufacturers to leave unique marks on ammunition. Some US states have already made micro-stamping a legal requirement for manufacturers of handguns.

Brain fingerprints

Brain Fingerprinting Laboratories, Inc. has developed and patented EEG/P300 testing systems that allegedly determines with accuracy whether specific information is stored in a person's memory. In a Brain fingerprinting test, relevant words, pictures, or sounds are presented to a subject by a computer in a series with irrelevant and control stimuli. The brainwave responses to these stimuli are measured using a patented headband equipped with EEG sensors. The data is then analyzed to determine if the relevant information is present in the subject's memory. A specific, measurable brain response known as a P300 is emitted by the brain of a subject who has the relevant information stored in his brain, but not by a subject who does not have this record in his brain. The technology is being used to improve security in areas like VISA applications and the protection of classified information and in the insurance industry.

English evidence law

Such bio-information and digital evidence can be used to build up a profile of a person. Such criminal profiling can breach Article 14, freedom from discrimination, which states:

"The enjoyments of rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or status."

Profiling cannot be used in court except as expert evidence

The expert evidence relating to areas of specialized knowledge such as:

- victimology,
- offence planning,
- modus operandi,
- motive, foresight, and

- issues relating to offender identity.

Profiling-Police Intelligence

The only other role of profiling[29] is police intelligence. The prosecution may decide to exclude some of the evidence gathered by the above techniques, relying on section 78 of the Police and Criminal Evidence Act.

Caselaw R v Stephen Craven

In the case of ***R v Stephen Craven***[30] the decision was that, for a safe conviction, the evidence must be considered in full but when not all of the evidence was considered, it did not mean that the conviction is unsafe. This is a strange rationale. C's appeal against conviction had been dismissed in 1993. The prosecution's case was that C had had an argument with the victim ('V') in a busy nightclub and had thrust a pint glass horizontally at V's throat, severing her jugular vein. V later died from loss of blood. V's friend ('S') then attacked C, who received hospital treatment to a cut on his left hand.

C denied having been involved in an altercation with V and claimed he had cut his hand on a glass when he was carrying several glasses and one of them had broken. However, although the Crown had failed to disclose that a fingerprint found on a piece of glass identified as the murder weapon did not belong to C or to any of the staff who could have handled the glass.

Standards of justice

When looking at the case as a whole, the evidence was that C had been involved in the fight and that his blood was found on S's shirt. There was also evidence of C's behaviour after the incident and of what he had said in police

interviews. **The court is saying here that the withheld evidence was not material[31].** However, a prosecution that withholds evidence requested by defendant, which, if made available, would tend to exculpate him or reduce the penalty, is actually shaping a trial biased against the defendant. Such non-disclosure casts the prosecutor in the role of an architect of a proceeding and this does not comport with standards of justice.

The fallibility of expert bite-mark and footprint evidence

The stories of US expert witness Michael West, a dentist and bite-mark expert from Mississippi and of Louise Robbins, a college anthropology professor and footprint expert, are not as well-known in the UK as are stories of the UK prosecution expert witness against Sally Clarke[32]. Footprint expert Robbins was an expert witness in more than 20 criminal cases in 11 American states and in Canada during a 10-year period. Michael West has been an expert witness in 55 cases in nine American states over 12 years, 18 of which cases were capital murder cases. He acts solely as a prosecution expert witness for bite-marks, matching wounds with weapons, footprints, shoeprints, fingernails with scratches, and spills with stains.

Matching fingernails to scratches on forearm

In 1990, West matched the fingernails of a murder victim to scratches on the forearms of the defendant, Mark Oppie. Also in 1990, West identified a footprint on a murdered girl's face in Jefferson Parish, near New Orleans, as having been made by an athletic shoe found in the apartment of a neighbour. In 1991, Michael West matched a bruise on a murdered boy's stomach to a hiking boot belonging to the boy's mother, Patricia Van Winkle[33]. In 1992, West positively identified a bite mark on an elderly rape and robbery victim in

Jackson County, Mississippi, as having been made by Bourn. However, hair and fingerprint evidence from the crime scene did not match the defendant's. The DNA analysis of the skin obtained from fingernail scrapings of the victim, positively excluded Bourn.

Mark Hansen[34] wrote, "The controversy over West's self-proclaimed expertise illustrates, at a state level, the types of issues that courts confront in deciding who qualifies as an expert witness and what constitutes scientific evidence". Yet, the US ruling in *Daubert v Merrell Dow Pharmacetuicals*[35] determines that evidence must be based on good grounds of what is known in a particular field; that the theory or technique can and has been tested; that testing must involve peer review and publication; that error rates and control techniques will affect admissibility; and that publication of a theory does not imply reliability.

Cross-border sharing of database information

There are many European Member States which can access each other's police databases through Interpol.[36] Any DNA profiles sent by UK police are *exempt* from the Data Protection Act 1998, in force in March 2000 and replacing the Data Protection Act 1984. There is no internationally agreed framework for sharing data. There is no oversight body to monitor the international exchange of DNA profiles, yet there is in place a centralised database of fingerprints across the whole of the European Union, with a proposed obligation on each Member State to transfer details held by national police forces to a central authority. The relevant laws are Title V1 of the Treaty on European Union which sets out the common interests which Member States agree to cooperate upon and the 2005 Prum Treaty signed by 11 Member States to agree to exchange information. This approach to such an important subject is astonishing

The moral of the story

Bio-information and digital information as evidence in English courts must be treated with extreme caution and not as the gung-ho acceptable without question it is still treated as today.

Bibliography

Editorial, "Unreliable evidence", New Scientist, 4 October 2008.

UKCLE, "When science doesn't meet the law: addressing the absence of forensic skills in law degrees", University of Warwick Press, September 2008

R. May, "Fair Play at Trial: an Interim Assessment of Section 78 of the Police and Criminal Evidence Act 1984", Criminal Law Review 723, 1988.

N. Ratha and R. Bolle**,** *Automatic fingerprint recognition systems*, (Springer, New York 2004).

J. R. Spencer, *Evidence of Bad Character*, (Hart Publishing, Oxford 2006).

R. Wilcock, R. Bull & R. Milne, *Witness Identification in Criminal Cases*, (OUP, Oxford 2008);

ENDNOTES

1. [1993] AC 593. This House of Lords decision is on the *use of legislative history in statutory interpretation*. The court established the principle that when primary legislation is ambiguous then, under certain circumstances, the court may refer to statements made in the House of Commons or House of Lords in an attempt to interpret the meaning of the legislation. This is known as persuasive authority (not defined in English law) but does not extend to somebody's article in the Criminal Law Review.

2. I have seen reference in a recent court decision to an article written by a writer in the "Criminal Law Review", a Thomson Reuters publication, and *not a parliamentary paper*. This *slippage of rules by judges* undermines the English justice system, creating a veritable "free for all- *anything goes*- as far as rules are concerned- and making a mockery of the *Criminal Justice Act 2003*.

3. His Honour Judge Waxse, "Digital Discovery & e-Evidence," (Pike & Fischer, Maryland, US 2007).

4. Noise is the value of processed information circulating in the intelligence system because information is graded along a spectrum of usefulness and because all information is subject to interpretation. For example, civilians make reports about firearms from time to time, but not all of these reports are of the same value. There is a lot of low-grade intelligence .This noise in an information system is related to the distance between the reporting, recording and interpretation of data. The greater the gaps between information reporting, intelligence analysis and dissemination, the greater the capacity for generating noise.

5. J.Sheptychi, "Organisational pathologies in Police intelligence systems", European Journal of Criminology, Volume 1(3), Sage Publications, 2004.

6. See http://www.sconul.ac.uk/activities/access/papers/dpa_checklist.doc

7.The use of interception powers is monitored by the Interception of Communications Commissioner whose annual reports to the Prime Minister are tabled in Parliament and then made available to the public. The expenditure, administration, and policies relating to interceptions for national security purposes are monitored by a statutory parliamentary committee. Members of the public can lodge complaints with the Investigatory Powers Tribunal, which has power to cancel warrants and award compensation. In recent years legislative amendments have been introduced to enhance the implementation of the interception law . Data retention powers given to the police recently are powers to record the transmission and not information on the contents of communications with the exception of parliamentarians' transmissions, which are protected by the "Wilson Doctrine".

8.Chapter 30. The Act received Royal Assent on 30 October 2007.

9.Prime Minister Blair's speech in February 2007.

10. Editor, "News in perspective", *New Scientist,* 24 February 2007, at page 4.

11. B. Hamilton and S. Cohen, "Clueless crime labs", New York Post, 21 Sept. 2008. A federal panel of experts looking into the reliability of CSI tests has heard damning evidence against some of the most common techniques used to convict killers, rapists and other criminals.

12. See US National Academy of Exports December 2008 Report. The survey was conducted from 2006 to 2008 by a top-slice team of 17 evaluators. This damning

report has great implications for guilt and innocence in US courts. The matching of bite marks, which involves using putty to preserve impressions and making moulds to reproduce suspects' teeth, has been shown as unreliable. Examiners in one of the Academy's evaluations falsely identified an innocent person as the biter 63 percent of the time.

13.R. Stone, "Exclusion of Evidence under Section 78 of the Police and Criminal Evidence Act: Practice and Principles", Web Journal of Current Legal Issues, 1995.

14.*Choiri v UK* [1999] ECHR App. No. 44926/98. See also *R v DPP, ex parte D.G. Duckenfield; B.D. Murray: R v South Yorkshire Police Authority; A. Addlington (on behalf of the Hillsborough Family Support Group); Duckenfield; Murray; Hillsborough Police Authority, ex parte Constable of South Yorkshire* [2000] 1 LR 55; [1999 2 All ER 873; Times, 21 April 1999.

15. [2004] EWHC 362 (Admin)

16. If on the other hand, he had disputed that he was the person that was disqualified, the procedures allowed to identify him include video-film identification and the police station video of his previous charge could have been used, with the claimant's consent (paragraph 2.1 of Code D).

The right to choose one's solicitor is not an absolute right and there would be no risk of injustice to the claimant if he were required to make a fresh choice of solicitor.

17. [2008] EWCA Crim 975

18. Under section 61(3) PACE, fingerprints of a person detained at a police station may be taken without that person's permission in two circumstances:- where an officer of at least the rank of inspector authorises them to be taken or where the person has been charged or reported for a

recordable offence and the person's fingerprints have not already been taken in the course of

the investigation of the offence by the police.

19. [2008] EWCA Crim 975

20. Court of Appeal, 2 December 1985

21. [2004] UKHL 39

22. [1982] 75 Cr App R 247

23. The scope for attaching consequences to foreign convictions was a matter for national law and was "often limited". A court in one Member State must be able to

take account of final criminal judgments rendered by the courts in other Member States for the purposes of assessing the offender's criminal record and establishing whether he has re-offended, and in order to determine the type of sentence applicable and the arrangements for enforcing it. This reads as being information relevant only to sentencing and not to trial.

24. Under s.7, Evidence Act 1851 the prosecution may rely on examined copies of convictions

to prove foreign convictions. In other words, the Evidence Act 1951 allowed documentary evidence from other jurisdictions, but not bio-information evidence.

25. [2001] EWCA Crim 571

26. *F. E. Barlow& D. W. Barlow v BOC Ltd &Edwards High Vacuum International Ltd* [2001] 3 WLR 168; Times, 10 July 2001; Independent, 15 June 2001. This fact goes deeper to the issue because the Rehabilitation of Offenders Act 1974 outlaws discrimination against ex-offenders. Pertaining only to convictions in the UK, most convictions become 'spent' after five years; prison sentences up to six months become spent after seven years; prison sentences up to two and a half years become spent after 10 years; sentences over 2.5 years are never spent and rehabilitation periods are halved if you were under 18 when convicted. There is nothing to stop an employee insistent of a finding of gross misconduct to gain access to foreign convictions obtained by a CPS's request under the Criminal Justice (International Cooperation) Act 1990.

27. *Re V: Re L (Minors) (Sexual Abuse: Disclosure)* [1999] 1 WLR 299, when leave to appeal to the House of Lords was refused. Disclosure about findings of sexual abuse in Children

Act cases should only be made where there was a pressing need. It is inappropriate to direct

disclosure of information about such findings unless the application came within the broad

principles set out in *Re C: (A Minor) (Care Proceedings: Disclosure*) [1997] 2 FLR 725.

28. See website PoliceOne.com news as at 08.10.2008.

29. Criminal profiling can breach Article 14; freedom from[1] Criminal profiling can breach Article 14, freedom from discrimination. "The enjoyments of rights and freedoms set forth in this Convention shall be secured without discrimination on any

ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or status."

30. Court of Appeal, 8 December 2000

31. The question of *materiality* is one of law to be determined by the court of trial (see s 1(6)). This subsection settles a point as to which some doubt attached. As to the term "materiality" see-

R v Philpotts (1851) 3 Car & Kir 135.

R v Gibbon (1862) Le & Ca 109;

R v Mullany (1865) Le & Ca 593;

R v Shaw (1865) Le & Ca 579, 29 JP 339;

R v Tyson (1867) LR 1 CCR 107, 32 JP 53;

R v Smith (1867) LR 1 CCR 110, 32 JP 405;

R v Alsop (1869) 33 JP 485;

R v Hadfield (1886) 51 JP 344*;*

R v Baker [1895] 1 QB 797;

R v Hewitt (1913) 9 Cr App Rep 192;

R v Wheeler [1917] 1 KB 283, 81 JP 75.

32. *R v Clark* [2003] EWCA Crim 1020 (11 April 2003).

In this case, *R v Sally Clarke,* involving the daughter of a police officer whose two babies had died inexplicably, and for which deaths she was charged, tried, convicted, imprisoned, and which was appealed years later due to new fact found that baby had had an infection [and she was thereafter released] expert witness Professor Meadow became discredited for the flawed statistical evidence that he gave in court because he gave evidence on a matter in an area in which he was not expert; his speciality was in paediatrics. The case 'raised hackles' and resulted in pertinent law articles, some of which the author cites here:

Editor, "A review of the current scientific status and fields of application of Polygraphic Deception Detection", *The British Psychological Society,* October 2004.

Editor, *"The old boys' club and its inexpert experts can still hold juries in thrall*", *Times Newspaper*, 13 January 2005.

Editor, "Sudden unexpected death in infancy: A multi-agency protocol for care and investigation", *The Royal College of Pathologists and The Royal College of Paediatrics and Child Health,* September 2004.

C. Pamplin, “Taking experts out of court”, *New Law Journal*, 26 Nov. 2004.

B. Thompson, *“*Expert Witnesses in the dock*”, The Barrister*, 2004.

I .Walker, “The Single Joint Expert-a leading solicitor's view,” *The Expert Witness Institute Newsletter*, Summer, 2004.

33. *State v. Van Winkle*, 658 So.2d 198 (Louisiana Supreme Court).

34. Mark Hansen, “Out of the blue”, *American Bar Association Journal*, February 1996.

35. Caselaw, United States, 113 S. Ct. 2786 (1993).

36. Paragraph 7.46 of “The forensic use of bio-information: ethical issues”, *Nuffield Foundation*, London 2007.

SALLY RAMAGE
ISSN series 1758-8421.