Title: **What makes you clever The puzzle of intelligence**

Author: **Derek Partridge**

Date and place of publication**: Singapore, 2014**

Publisher: **World Scientific**

ISBN: **978 9 8145 1304 3** (paperback)

This is a book on how people working on software code in an attempt to produce Artificial Intelligence (AI) (whatever that is) have consistently failed, despite the inaccurate hype in the media.

This book is relevant to lawyers because the author takes a careful look at what intelligence might be considered to be, and the different approaches used by people working on writing software code to replicate their view on what they consider intelligence to be. The significance is that Professor Partridge demonstrates that every attempt by human beings to write software code and algorithms to produce something called AI has failed. This is partly because of the methods adopted to understand human intelligence, but largely because of the nature of intelligence itself – complex and nebulous. It is also because of the complexity of the software code and the systems such code needs to operate on. The conundrum is neatly revealed in footnote 15 on page 23:

> 'Although I'd advise strongly against delaying purchase of your next computer system until the "intelligence" utility is available, it's an intriguing idea. For example, would your "intelligent" laptop immediately dump your Microsoft systems and start searching the Internet for something more secure?'

Of immediate importance to lawyers are the observations regarding fMRI and other neuroimaging technologies that purport to correlate regions of brain metabolic activity with particular cognitive functions (chapter 3), and mention is made of the book *Brainwashed: The Seductive Appeal of Mindless Neuroscience* by Sally Satel and Scott O. Lilienfeld (Basics Books, 2013) that sets out the details of brain scanning and why, and in what ways, it is misused to explore what we are thinking. Taking into account Professor Partridge's observations in footnote 13 on page 107 regarding the book by Steven Pinker, *How the Mind Works* (Penguin, 1998), it would be helpful for lawyers advising in medical issues to be aware that we do not know much about how the mind works:

> '[*How the Mind Works*] … is replete with vague claims … which give the impression that we know quite a lot about how the mind works, but boils away to almost nothing once an effort is made to pin down details.'

Of importance to all lawyers is the presumption in England and Wales, that: 'In the absence of evidence to the contrary, the courts will presume that mechanical instruments were in order at the material time.' The Law Commission formulated this presumption in 1997 (The Law Commission, *Evidence in Criminal Proceedings: Hearsay and Related Topics* (1997), 13.13. It is assumed (and the decisions of judges reinforce this assumption), that 'mechanical instruments' include computers and computer-like devices. The failure of the Law Commission to provide any technical reasons why such a presumption can be sustained; the assumptions adopted by judges about the 'reliability' of computers generally (if so, why the panic over the relatively trivial century date change?), and a detailed illustration as to why the technical evidence contradicts the legal assumption is discussed in detail in chapter 5 of Stephen Mason, gen ed, *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012).

The observations by Professor Partridge bear directly on the difficulties of this presumption, where he says this on page 203 (emphasis in the original):

> 'One thing that the software engineer would like to be sure of when struggling to get a conceptual grasp of an IT system (whether he originally wrote it, or not) is that the program *as written has not changed*. The original programming was presumably based on an explicit design with certain (hopefully, also well documented) goals, and was tested thoroughly. But if that's all changed because the system has learned from its experiences, the software engineer's already unmanageable task has escalated. The difficult job of interpreting somebody's best efforts has escalated by the additional need to also interpret a learning algorithm's actions.

> The learning process will have introduced changes as a result of the details of the system's history. What changes have been made, and how exactly they have been introduced is dependent on the details of the learning algorithms. Unraveling this degree of indirect consequences in an IT-system's innards threatens to ... to? Words fail me.'

Taking into account that what is described already occurs, but not necessarily by algorithms, it has to be a surprise that the law in England and Wales continues to support a presumption that cannot be sustained by any evidence.

As pointed out on page 394, no significant program is completely understood, and the observation on this point, discussed in more detail on page 407 and pages 426 – 428, is illustrated by the RBS bank IT system failure of June 2012 (for which see footnote 22 on page 415).

What makes this book of interest to practicing lawyers is the demonstration that AI is far from being any sort of 'reality' and software code cannot remotely be considered to be 'reliable' in the context of a legal presumption – that in itself is merely a shorthand to allow evidence from machines to be admitted into evidence (sometimes in the most dubious of cases, especially banking cases), regardless of the fact that the technical reality does not accord with the justification for a presumption.

Title: **Evidentiary Foundations**

Author: **Edward J. Imwinkelried**

Date and place of publication**: San Francisco, 2015**

Edition: **9th**

Publisher: **LexisNexis**

ISBN: **978 1 63281 546 1** (softback)

This useful text first prepared in 1980 to help law students develop a working understanding of the evidentiary doctrines discussed in the classroom. There do not appear to be any comparable textbooks covering the same material in the jurisdictions comprising the United Kingdom, and it may be that there are few other jurisdictions that have similar textbooks.

The marketing text on the LexisNexis web site sets out what the book aims to accomplish:

> 'This time-tested evidence treatise covers all the major evidentiary doctrines, and includes expert analysis of statutory developments along with discussions of the presentation of hard copy exhibits in court using document cameras and the presentation of digital exhibits using monitors or projection screens. Detailed explanations of evidence principles include:
>
> > A brief description of the pertinent Federal Rules of Evidence and the most recent leading cases construing the Rules.
> >
> > A list of foundational elements-the events and facts you need to lay a complete foundation.
> >
> > An illustrative foundation showing how each question relates to a particular element of the foundation.
>
> The Ninth Edition introduces new coverage on topics such as scanned documents, learned treatises and ancient writings. In addition, in light of advancing technology, the Ninth Edition updates the foundations for audiotapes, videotapes, and automated surveillance cameras.'

Apparently over 125,000 copies have been sold during the life of the text. It is not without reason that such sales figures have been achieved: the book is a helpful guide to the aspiring lawyer that intends to be an advocate. The contents are as follows:

Chapter 10 The Hearsay Rule, Its Exemptions, and Its Exceptions

Chapter 11 Substitutes for Evidence

For the purposes of this review, consideration is only given to those parts of the text that are relevant regarding electronic signatures and digital evidence.

Of particular interest are the discussions regarding chapter 4 and authentication. The coverage includes print-outs from a social media profile page (4.02[6]), indicating that there are no set rules for the authentication of such evidence; e-mail (4.03[4][a]); scanned documents (4.0[5]); information posted on the web site of a business (4.03[6]), self-authenticating business records (4.03[7]), and computer animations and simulations (4.09[5][a]) – although there does not seem to be, sadly, a reference to the most important textbook on this topic, namely Gregory P. Joseph, *Modern Visual Evidence*, Law Journal Press (looseleaf).

An issue of significance relates to computer records (4.03[2]). It is with the eleven part test relating to computer records that there is some difficulty, as explained in Stephen Mason, gen ed, *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012), 4.24:

> 'The steps outlined by Prof. Imwinkelried are helpful, but item 1 is hardly a ground for admitting digital data, in that software in computers and computer-like devices are put on the market when a manufacturer is satisfied that such devices will sell, not that they are reliable or can be trusted to be accurate. Item 2 is impossible to demonstrate, and item 5 is prone to being undermined by the failure of an organisation to consider such issues when operating their computers, although it is debatable whether the concepts of a computer being reliable or in a good state of repair are helpful (or relevant) in understanding whether a computer was working properly – and the term 'working properly' is also to be questioned.'

The observations noted above have been part of *Electronic Evidence* since the first edition in 2007, and Professor Imwinkelried is urged to consider revising this list, given the extensive treatment of this topic in chapter 5 of *Electronic Evidence*. The Professor notes that under Federal Rule of Evidence 201, the trial judge has the ability to judicially notice the validity theory underlying computers and the general reliability of computers. The only problem regarding the 'reliability' of computers or computer-lie devices is that such a term is not relevant to computers. Naturally, where the output of a computer is not disputed (especially in civil litigation), it seems perverse and a waste of time and money to authenticate any form of evidence – including digital evidence. However, the significant problem is when the party challenging the evidence from a computer or computer-like device does so on the basis that the output is incorrect. This occurs reasonably often, particularly in speeding cases, and Professor Imwinkelried is encouraged to reconsider the points made in *Electronic Evidence*.

Digital signatures are discussed at 4.03[4][b] and 4.03[4][c]. The text deals with testimony about a digital signature at 4.03[4][c][iii]. Of interest are the model questions and answers towards the end of the exercise, which also raises an important problem. The first is the end of the testimony from an expert, in which they explain how the public key infrastructure works. The text concludes as follows (italics added):

> W You get another hash number. If the two numbers match, now Recipient can conclude that no one has tampered with the text of the message. If no one has tampered with the text of the message and the CA's certificate establishes that Sender holds that public key, *Recipient will conclude that he or she has an authentic message from Sender*. If that message is a purchase order for a certain number of goods, now *Recipient can rely* on the order and get ready to ship to Sender.

The second is the latter part of the testimony from a witness that explains how the technology was used:

> W I got a hash number.
>
> P WHAT did you do next?
>
> W I independently hashed the text of the message that purported to come from Martinez Corporation.
>
> P WHAT happened when you did that?
>
> W I got another hash number.
>
> P HOW did the two numbers compare?
>
> W They were identical.
>
> P At that point, WHAT did you conclude?

W That the message *had in fact* come from Martinez Corporation.

The words in italics illustrate a false impression invented by technicians, called 'non-repudiation'. The technicians would like it to appear that the sender cannot deny they sent the message – and the text illustrated in italics illustrates this misleading assertion.

This assertion is incorrect, as explained in detail in Stephen Mason, *Electronic Signatures in Law* (3rd edn, Cambridge University Press, 2012), 318 – 325, and as the Russian digital signature cases illustrate, for which see: Russian Federation Case Note: Case A12-3342/05-C11, The Federal Arbitration of the Povolzhsky District, 4 *Digital Evidence and Electronic Signature Law Review*, (2007) 83 – 85; Olga I. Kudryavtseva, 'The use of electronic digital signatures in banking relationships in the Russian Federation', 5 *Digital Evidence and Electronic Signature Law Review*, (2008) 51 – 57; Olga I. Kudryavtseva, 'Resolution of the Federal Arbitration Court of Moscow Region of 5 November 2003 N КГ-А 40/8531-03-П', *Digital Evidence and Electronic Signature Law Review*, 5 (2008) 149 – 151.

The fact is, as explained by Mason at 324:

> '… that this technical concept relates to events that have taken place after the signature has taken place, and has no relation to the actual mechanism of the affixing of the digital certificate.'

Others make this elementary mistake, including, more recently, Professor Dr. Christoph Sorge in his article 'The Legal Classification of Identity-Based Signatures' in *Computer Law & Security Review*, Volume 30, Issue 2, April 2014, 126 – 136, where he states, at 126 'Non-repudiation is also achieved, i.e. it can be proven that the message was signed by the signatory.'

It is sincerely to be hoped that future editions of this excellent text reconsider the issues noted above.

Finally, mention of the proof required for a biodynamic version of a manuscript signature will act to help lawyers significantly – especially in the United States of America, where this text is sold, and where such methods of electronic signature are widespread. At present it seems as if lawyers consider it relevant, when proving and challenging the biodynamic version of a manuscript signature, to ask a handwriting expert to make a comparison between two completely different forms of evidence: a manuscript signature and a digital representation of a signature made using a pen and a pad. The fact is, that this is an inaccurate method of determining whether such an electronic signature was effected, as indicated by Heidi H. Harralson in her article 'Forensic document examination of electronically captured signatures', 9 *Digital Evidence and Electronic Signature Law Review* (2012) 67 – 73.

This is a helpful and influential text.

Title: **Math on Trial How Numbers Get Used and Abused in the Courtroom**

Authors: **Leil Schneps and Coralie Colmez**

Date and place of publication**: New York, 2013**

Publisher: **Basic Books**

ISBN: **978 0 465 03292 1**

One of the worst uses of the incorrect calculation of statistics in criminal trials in England and Wales concerned the alleged murder of babies by their mothers. The most high profile was that of Sally Clarke. Justice was eventually done and seen to be done, but not after hundreds of families were charged with the murder of their babies. The authors set out 10 errors and highlight each error with an account of a criminal case or set of facts that illustrate the error. They are:

Multiplying non-independent probabilities (Sally Clark)

Unjustified estimates (Malcolm and Janet Collins and identity)

Trying to get something from nothing (Joe Sneed and the murder of his parents)

The failure to order a second experiment (Amanda Knox and the misunderstanding of probability led the judge to discount critical evidence)

The birthday problem (the murder of Diana Sylvester and the use of probability to convict years later)

Simpson's paradox (sex bias cases at Berkeley)

Incredible coincidence (Lucia de Berk, accused and convicted of murder because of coincidence)

Underestimation (Charles Ponizi and misunderstanding exponential growth)

Choosing a wrong model (Hetty Green and the dispute over her aunt's will)

Mathematical madness (Alfred Dreyfus and the specious deduction made by Alphonse Bertillon)

The improper application of mathematical concepts can mean the difference between an educated prosecutor considering the evidence before a person is charged with an offence and deciding not to rely on the improper use of mathematics and the humiliation of being publically proved ignorant. For the individual that is accused, it usually means not being wrongly accused of an offence that there is no other evidence to convict.

Two observations merit comment:

1. Malcolm Collins appealed against conviction to the Supreme Court of California. Laurence Tribe (presently the Carl M. Loeb University Professor at Harvard University), at the time a clerk assisting one of the judges at the court, had majored and excelled in mathematics at Harvard before attending law school (a good argument to adopt the US requirement that lawyers can only qualify if they have a degree in another subject before law). He wrote a memorandum for one of the judges that systemically set out all of the errors relied upon by the prosecution. The question is, what was the probability that Laurence Tribe would be in the right place at the right time to ensure that the appellate judges were not swayed by poor mathematics?

2. In the case of Lucia de Berk, Henk Elffers, a professor of law and psychology who specialised in the psychology of compliance and spatial crime analysis, gave evidence regarding statistical reasoning. As the authors point out, the Netherlands is not short of internationally renowned professors in mathematical statistics, yet the lawyers and the judge accepted professor Elffers as an expert witness. The questions are: why did the professor agree to provide expert evidence in a topic of which he was not, apparently, qualified? Why did the prosecution ask him to give evidence? Did the defence lawyers object? If not, why not? Why did the judge accept his qualifications?

This book by Leil Schneps and Coralie Colmez, members of the Bayes in Law Research Consortium, an international team dedicated to improving the use of probability and statistics in criminal trials, should be compulsory reading for every aspiring lawyer.

Title: **The Seductive Computer Why IT Systems Always Fail**

Author: **Derek Partridge**

Date and place of publication**: London, 2011**

Publisher: **Springer-Verlag**

ISBN: **978 1 84996 498 2** (paperback)

Professor Partridge has written an eminently readable text on why writing software code is so difficult, which leads to the observation, on page X, that:

> 'What you are unlikely to know is that all these computer systems are, and will always be, imperfect, which is a polite way to say that they contain errors and will thus go wrong – sometimes irretrievably so. All IT systems will sometimes fail.'

In this book, Professor Partridge sets out to demonstrate that the fundamental problem is complexity, which leads to 'unavoidable unmanageability'. It is this 'unmanageability' that is analysed and explained in this text. Although the analysis is primarily technical in nature, nevertheless the reader with no interest in how software code is written and works (including the author of this review), will find that Professor Partridge has taken great pains to make the book relatively easy to understand for the non-technical reader without being condescending.

At present, lawyers and judges either have a blind acceptance of the 'reliability' of computers (in actuality, software code, IT systems) – without defining what 'reliability' means – or ignore the technology to such an extent that some judges have made comments in judgments that are patently incorrect.

Detailed consideration is given to how software code is written, conceptualised and managed. In addition, discussion is given to the various methods put forward to try and prove that a program is, in general, correct

– including why it is not possible to import mathematical certainty or demonstrate proof of correctness – even with, for example, software code that is responsible for flying aircraft (page 224). At one place (page 112), Professor Partridge makes an important point that lawyers and judges ought to be aware of when dealing with banking cases:

> 'So we can't prove that the bank's computer always computes the balance of our accounts correctly, but if it doesn't it must be simply because some programmer gave it a wrong instruction. Computers only do what they are told, so why don't we just make sure that we tell them what to do correctly? Why indeed?'

The central point is, as indicated in bullet points at the end of a chapter on pages 127-128, is:

> 'Computers most assuredly do only what we tell them to do.
>
> What we've told a computer to do must be distinguished from what we believe we've told it to do.
>
> Knowing what you've told a computer to do is impossible to establish with certainty.'

The book offers a balanced approach to the myriad problems relating to writing software code and the problems associated with complex systems, and discusses potential technical solutions in part III. In chapters 24 and 25 provide a very useful précis of the problems, making it clear that the software code we rely on every day is flawed and will always be so, but a change in attitude to how software code is written can ameliorate the problem, but will never eliminate software failures.

Title: **Electronic Disclosure A Casebook for Civil and Criminal Practitioners**

Author: **Stephen Mason**

Date and place of publication**: St Albans, 2015**

Publisher: **PP Publishing**

ISBN: **978 1 858 811 6068**

eBook: **978 1 858 811 6075**

Electronic disclosure, or eDisclosure, is now the every-day fare of all practicing lawyers in England and Wales, in the same way as electronic evidence and electronic signatures. Lawyers now deal with the complexities of these topics every day. Litigation and eDisclosure now go hand-in-hand.

Although the members of the judiciary took up the challenge and set out guidance and rules relating to eDisclosure some years ago, nevertheless, the case law suggests that many lawyers remain blissfully unaware of these three important topics: eDisclosure, eEvidence and eSignatures.

The aim of this concise guide is to set out the case law relating to eDisclosure in England and Wales, and to indicate how judges have approached the problems of eDisclosure in both civil and criminal proceedings. This work does not purport to be comprehensive.

Contents

Title: **Electronic Contracts**

Author: **Simon Blount**

Date and place of publication: **Australia, 2015**

Edition: **2nd**

Publisher: **LexisNexis Butterworths**

ISBN: **9 780 409 340 747** (paperback)

e-book: **9 780 409 340 754**

(Late arrival)

Contents

From the LexisNexis web site:

In this new edition, Dr Blount continues his scholarly and very valuable contribution to this emerging area of the law. The significance of a text like this, that synthesises the law and categorises issues that arise in an area vital to our daily lives, cannot be understated.

From the foreword to the first edition by the Honourable Justice Steven Rares J.

This book identifies issues of contract law that are uniquely problematic for electronic contracts, such as whether clicking an 'I agree' box is really an acceptance of the terms of a contract, whether acceptance of an offer by email or text message attracts the postal acceptance rule, whether notice of terms can be given by hyperlink, and whether a term of 'fit for purpose' can be implied at common law for the download of software. In addition to considering the when, where and how of electronic contract formation and the incorporation and vitiation of webpage terms, the book analyses a large number of important common law appellate and superior court decisions to predict the likely law of electronic contracts for all common law jurisdictions, including Australia.

Expanded to cover the new developments in this area this second edition includes a new chapter on international conventions and model laws.

This book will be of immeasurable assistance to legal practitioners litigating and drafting electronic contracts, as well as to practitioners, academics, and students interested in the legal problems arising from the new information technologies.

Features:

- A detailed and scholarly coverage of the topic
- Applies a comparative approach
- The author considers over 150 common law electronic contract cases at appellate level