Title: **Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor**

Author: **Virginia Eubanks**

Date and place of publication: **2018, New York, United States of America**

Publisher: **St Martin's Press**

ISBN: **978 1 250 07431 7** (hardback);
987 1 4668 8596 7 (e-book)

Professor Eubanks has researched and written about how people in control use software to 'provide' services – in the context of this book, to the poor in American society. By 'providing' is actually meant to control, punish and reduce the amount spent on the poor – at least this is the hidden agenda.

Professor Eubanks demonstrates how systems are set up in such a way that the humans that interact with applicants are probably instructed to ensure the process is opaque, meaning that when a form needs to be signed, the applicant is not told that a signature is required, or what form needs to be signed, or where to take the form. Examples abound.

People are denied help when they need it. Franz Kafka would recognize the world revealed in this book: a decision rejected? Appeal, but we prefer you not to appeal. We prefer you to resubmit the application. Why? It implicitly means you were wrong to make the first application, and by appealing the failure to give you help from the first application will mean you will not get help until the next phase of the application process begins.

The value of this book is the research that Professor Eubanks has undertaken. She has spoken not only to people that have been the subject of such unfairness, but also to those involved in the decision making process, using the software. Contradictions proliferate, but what is made clear is the explicit aim of saving money and the implicit aim of reducing the number of people receiving help.

This is a book that decision makers ought to read, but they probably do not need to – they know what they intend to achieve by commissioning such programs. Software is used as a deliberate method of ridding the morally suspect from hand-outs, and the police use the databases as a means of tidying up the homeless and those on the periphery of society.

Software kills and injures people (for which see chapter 6 of Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017)), and now we have excellent evidence that it also ensures people are prevented from receiving help – yes, software can also improve some decision making, as indicated by the author, but using software systems in the absence of increasing funding will not help those most in need.

Title: **The Secret Barrister: Stories of the Law and How It's Broken**

Author: **The Secret Barrister**

Date and place of publication: **2018, London**

Publisher: **Macmillan**

ISBN: Paperback **978 1 5098 4110 3**

All legal systems have flaws, and it often takes an outsider to notice the obvious. If you are part of the system, you know what the problems are, but live with them and occasionally try to improve how things work. The author of this book does an excellent job of exposing the weaknesses of the system of criminal justice in England and Wales from the perspective of a practicing barrister.

None of the examples of poor practice are new to the reviewer, who practiced in the criminal courts for a brief two year period in the late 1980s. The Keres example (p 187) brought back a memory where a notorious firm of solicitors instructed the reviewer to

attend a crown court plea without sending an instructing solicitor. This caused serious problems, because the client was particularly difficult, and the reviewer had to ask the advice of the prosecuting barrister and judge in chambers about finding a neutral third party to be witness to the confidential discussions with the client. The failure to be paid (p 193) is also not new. What has changed is the remorseless reduction of funding in the criminal justice system – so much so that the problems in the system are exacerbated because, arguably, spending is now so low as to seriously affect the central concept of criminal justice (see p 130). For a indication that this is not new, see Stephen Mason and Nicholas Bohm, 'Written evidence submitted to the Treasury Committee', 17 January 2011 https://publications.parliament.uk/pa/cm201011/cmselect/cmtreasy/430/430vw25.htm. This article was subsequently published with no changes to the conclusions: 'Banking and Fraud' *Computer Law & Security Review*, 2017, Volume 33, Issue 2, 237 – 241.

The author certainly asks the question that ought to be uppermost in the minds of many: why do people not seem to care (p 14)? This is an important point to make. The late Sir Nicholas Lyell informed the reviewer on one occasion that politicians do not take up an issue unless they receive regular correspondence on a particular topic. This might explain why MPs do not deal with this important issue (p 137), although it does not account for the failure of the media generally to consider the grave issues that arise from this book (but the discussion at pp 304 – 305 might explain this).

Interestingly, the author cites a paper from 2016 that suggests 'sleepy Monday' might cause a change in sentencing. For the record, another study was conducted by Shai Danziger, Jonathan Levav and Liora Avnaim-Pesso, 'Extraneous factors in judicial decisions', *PNAS*, 26 April 2011, Volume 108, Number 17, 6889 – 689. The findings were criticized by Keren Weinshall-Margel and John Shapard, 'Overlooked factors in the analysis of parole decisions', *PNAS*, 18 October 2011, Volume 108, Number 42, E833, and Andreas Glöckner, 'The irrational hungry judge effect revisited: Simulations reveal that the magnitude of the effect is overestimated', *Judgment and Decision Making*, Volume 11, Number 6, November 2016, 601 – 610.

The myth of state impartiality, at pp 261 – 270, is interesting and no doubt relevant, but examples of bad investigations and prosecutions ought to be cited to sustain the arguments. The reviewer recently went to a Member State of the European Union to conduct two courses, each of two days, to teach electronic evidence to judges, lawyers, prosecutors and police investigators. It transpired that in accidents involving motor vehicles, the police in this Member State are still not aware that motor vehicles no longer rely on physical rods to brake, but ABS. This ignorance is to the detriment of those accused of failing to brake when they have done so. It is to be guessed that this particular State is no different to many others across the globe, not just the European Union. This is a seriously frightening situation to find ourselves in, especially where politicians the world over are vying to permit motor vehicles controlled by inadequate software to control motor vehicles, and this especially important give that judges are notorious for refusing to permit software code to be reviewed (there is one exception, set out in chapter 6 of *Electronic Evidence*).

In setting the scene, the author refers to the need for the trier of fact to base their verdict on sound evidence (p 45), and the need for critical thinking is mentioned on p 70. Yet the text is peppered with signs that evidence in electronic form does not come within the purview of this author. Electronic evidence is now crucial in the vast majority of cases, especially vehicles, yet overwhelming numbers of lawyers are not even aware that the only up-to-date book on the topic is now in its fourth edition (Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017) and a free download as open source: http://ials.sas.ac.uk/digital/humanities-digital-library/observing-law-ials-open-book-service-law/electronic-evidence. This is important, as the text of chapter 6 explains and illustrates that few lawyers

or judges are actually exercising critical thinking when it comes to such an important aspect of contemporary evidence, especially over the irrational presumption that computers are reliable, although the position is even more absurd, for which see Stephen Mason, 'Artificial intelligence: Oh really? And why judges and lawyers are central to the way we live now – but they don't know it', *Computer and Telecommunications Law Review*, 2017, Volume 23, Issue 8, 213 – 225, 222:

> 'The presumption also illustrates the hypocrisy at the heart of English law. Lawyers write clauses for contracts relating to the use of software code that require the user to accept that the software is not free of errors. Such contract terms are considered so normal that nobody appears to understand this fundamental contradiction between the presumption and the acceptance of flawed software code as being normal.'

If a barrister is to take work beyond their competence (p 322), it is about time that the profession woke up to the need for education in this important topic (the journal has published articles on the need for education, for which see Denise H. Wong and Deveral Capps in volume 10 (2013) – including a free syllabus – but nothing has been done anywhere to rectify this serious failure).

The importance of forensics is mentioned (pp 259 – 260), and the need to obtain an appropriately qualified and knowledgeable witness is crucial, yet it is amazing that judges let lay people give evidence on matters that they are not qualified to do, for which see chapter 10 of *Electronic Evidence*.

The author finishes, on p 340, with the statement that 'my naïve, hopeless hope is that we might one day re-imagine functioning, accessible criminal justice as a comparably vital policy of universal insurance.' To add to this wish, this reviewer also hopes that the author of *The Secret Barrister* will begin to appreciate that the topic of electronic evidence, ignored by judges and lawyers for so long, is a significant part of this process.

Title: **Electronic Discovery and Digital Evidence in a Nutshell**

Author: **Shira A. Scheindlin and The Sedona Conference**

Edition: **Second**

Date and place of publication: **2016, United States of America**

Publisher: **West Academic Publishing**

ISBN: **978 1 63459 748 7**

This book is dedicated to the late Richard G. Braman, who was a founder of the Sedona Conference. Mr Braman understood that the world was changing rapidly, and the law was as affected as any other part of the life in which we have begun to take for granted. In addition, Shira A. Scheindlin, a highly distinguished judge of the United States District Judge of the United States District Court for the Southern District of New York, now retired, was also in the forefront of electronic discovery in the United States of America.

This excellent *Nutshell* is a very good guide not only for US practitioners, but for lawyers in other jurisdictions that wish to begin to understand the basic issues relating to these topics. This book compliments the text by George L. Paul, *Foundations of Digital Evidence* (American Bar Association 2008), and the practitioner book edited by Stephen Mason and Daniel Seng, *Electronic Evidence* (4th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017) and a free download as open source: http://ials.sas.ac.uk/digital/humanities-digital-library/observing-law-ials-open-book-service-law/electronic-evidence .

There are, however, a number of quibbles of this book that might appear to be minor in comparison to the content this excellent text, but are highly significant. Consider metadata. The authors indicate that in certain circumstances, metadata can be significant when determining authentication. This is, of course, correct. However, the authors state (p 66) that metadata 'is information about a particular data set that describes how, when and by whom it was

collected, created, accessed, modified'. With the greatest possible respect to the authors, this is not accurate. Metadata is *capable* of providing such information, but it does not follow that metadata has not been altered, removed or otherwise altered (see also p 214 – it can provide evidence of *purported* authorship).

The internet protocol address (IP) is another example. The discussion (p 93) of *Columbia Pictures Industries v. Bunnell*, 2007 WL 2080419 (C.D. Cal. May 29, 2007) illustrates another problem: Magistrate Judge Chooljian, noted, in footnote 7 (citing other authorities) that, 'An IP address is a standard way of identifying a computer that is connected to the Internet.' But this is also not necessarily correct. An IP address is *capable* of so doing, but with 200 users using the same IP address at any one time, by way of example (which is normal with IPv4), all that can be ascertained by an ISP is that *one of 200 users* were using a particular IP address at any one time.

The word 'reliable' is used to describe computer programs (p 414); 'reliable results' is also used (p 427); and in relation to business records, 'reliability and trustworthiness' (p 430), and 'sufficiently accurate' (p 416). As readers of chapter 6 of *Electronic Evidence* (4th edition) will be aware, the 'reliability' of software code is not proven, and the presumption of 'reliability' has never been defined by any judge anywhere (if there is a definition, the reviewer will appreciate notification). In addition, chapter 7 of *Electronic Evidence* argues that the business records exception should no longer apply – as the vignette 'Business records' illustrates at pp xii – xii in the same text. In addition, the work of Ken Chasse (see the *Digital Evidence and Electronic Signature Law Review* and citations of his work in *Electronic Evidence*) illustrates the significant evidential problems with accepting business records in electronic form.

Reference to the case of *U.S. v. Chiaradio*, 684 F.3d 265 (1st Cir. 2012) (pp 413 – 414) and 'reliable' (noted above) refers to a software tool called 'LimeWire' which was further developed by the FBI for their own purposes. The defence requested discovery of the source code (at 276). The purpose was set out at 277:

> 'The defendant argues that he had to obtain the source code in order to determine whether he could credibly challenge the reliability of the technology and, thus, block the expert testimony proffered by the government on the EP2P program and how it implicated the defendant.'

A *Daubert* hearing was held, and the District Court denied the motion to compel discovery of the source code. The Appeal Court agreed with the District Court, and indicated that the agent using the software program had no error rate, and demonstrated how the results of an investigation could be independently verified, and that the software had never yielded a false positive. The court considered that this evidence alone provided sufficient evidence of the reliability of the tool. The defence cited the lack of a peer review to challenge the software, but the Appeal Court indicated that the *Daubert* factors were not a definitive checklist, and there was a sound explanation for the absence of peer review (at 278):

> 'The record shows that the source code is purposely kept secret because the government reasonably fears that traders of child pornography (a notoriously computer-literate group) otherwise would be able to use the source code to develop ways either to evade apprehension or to mislead the authorities. This circumstance satisfactorily explains the absence of any peer review.'

In this case, the courts had more detailed evidence upon which to determine the questions raised, and is a more credible approach to the issue of the 'reliability' (whatever that means) than the approach taken by the Court of Appeal of Western Australia in the case of *Bevan v The State of Western Australia* (for which see *Electronic Evidence*, 6.45 – 6.55).

These are serious issues of evidence, and the authors indicate that attorneys have been disciplined for failing to be aware of the issues faced by lawyers in the digital age (e.g. p 60). Lawyers ought to have the necessary skills (p 129) to practice in the twenty-first century, and arguably, they ought also to have

knowledge of the important issues covered by this text. Judges have expressed their displeasure for the failure of lawyers to understand what they are supposed to be doing (pp 156 – 157). The authors point out that the American Bar Association has a set of Model Rules of Professional Conduct (amended to August 2012 at the date of this book). Rule 1.1 deals with competence:

> A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

This requirement is sufficiently wide to include competence and knowledge in discovery and electronic evidence – yet the reviewer is not aware of a single university or legal vocational course that teaches either topic. Members of the public should take note.

On a minor note, the authors discuss e-mails and evidence of receipt and sending. On pp 434 – 435, the following observation is made: 'The email contained the sender's typewritten name or nickname, or initials, or electronic signature'. A cursory study of *Electronic Signatures in Law* (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016), and a free download as open source: http://ials.sas.ac.uk/digital/humanities-digital-library/observing-law-ials-open-book-service-law/electronic-signatures, will indicate that the sender's typewritten name or nickname, or initials are all forms of electronic signature.

With the exception of the issues noted above, this book is a very useful guide to the law relating to disclosure and electronic evidence at the Federal level in the United States of America, and is recommended.

Title: **The Digital Ape how to live (in peace) with smart machines**

Editors: **Nigel Shadbolt and Roger Hampson**

Date and place of publication: **Australia and the United Kingdom, 2018**

Publisher: **Scribe publications**

ISBN: Hardback: **(UK) 978 1 91134 452 9**

The marketing blurb to his book offers a reasonable indication about the content:

> The smart-machines revolution is re-shaping our lives and our societies. Here, Nigel Shadbolt (one of Britain's leading authorities on artificial intelligence) and Roger Hampson dispel terror, confusion, and misconception. We are not about to be elbowed aside by a rebel army of super-intelligent robots of our own creation. We were using tools before we became *Homo sapiens*, and will continue to control them. How we exercise that control — in our private lives, in employment, in politics — and make the best of the wonderful opportunities, will determine our collective future well-being.
>
> Lucid, well-informed, and deeply human, *The Digital Ape* offers a unique approach. The authors prefer to add augmented wisdom to artificial intelligence.

The authors balance the ridiculous position taken by those that assume machines controlled by software code will take over the world against suggestion as to how such technology should be monitored and regulated.

As a book covering the topic in general terms, it is of interest. The discussion of 'the illusion of explanatory depth' (42) demonstrates the problems of the digital age: people just do not understand that they do not understand. In passing, it will be interesting to know why so many colloquial phrases were used – noticed by this reviewer after page 97 because of 'kettle of fish', followed by 'brought back from the brink' and 'trample on the hopes' (99); 'already in the can' (162);

'on the stocks' (166); 'tad' (170); 'the game … is worth the candle' (190); 'by a long chalk' (201); 'some mileage' (226); 'step up to the plate' (243); 'a bunch of' (257); 'cut and come again cake' (259) – whatever that means; 'two shakes of a lamb' (278).

Referring to Vannevar Bush predicting the World Wide Web in 1945, the authors might like to know that E. M. Forster also foresaw the internet in 1909 in 'The Machine Stops', a short story published in *The Oxford and Cambridge Review* (November 1909), republished in *The Eternal Moment and Other Stories* (1928), and again in *Collected Short Stories* (Penguin, 1954).

The discussion of the crisis of 2008 touches upon some of the important issues, including (25, 248) citing Gillian Tett, but fails to inform the reader of the software errors that were known at the time and were deliberately retained to produce false results (for which see Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017), 6.131-6.133). It also fails to indicate the simplicity of the problem: why would anybody think there is value in a bond that in turn comprises rights to a number of mortgages that everyone knows will never be paid? This problem was obvious in 2001.

The authors assert that the technology regarding mobile telephones is accurate, allowing the geographical position of a device to be ascertained with precision (26). A glance at the articles by R. P. Coutts and Hugh Selby will demonstrate that the technology is not quite as correct as assumed: 'Problems with cell phone evidence tendered to 'prove' the location of a person at a point in time', 13 *Digital Evidence and Electronic Signature Law Review* (2016) 76 – 87; ''Mobile Ping Data' – Metadata for Tracking', 14 *Digital Evidence and Electronic Signature Law Review* (2017) 22 – 25.

Worrying about natural stupidity is correct (56), especially the ridiculous presumption in law the computers are reliable, for which see *Electronic Evidence*, chapter 6 and Stephen Mason, 'Artificial intelligence: Oh really? And why judges and lawyers are central to the way we live now – but they don't know it', *Computer and Telecommunications Law Review*, 2017, Volume 23, Issue 8, 213 – 225. The law is hardly fit for purpose (298), especially when people begin to realise that not a single lawyer qualifying anywhere in the world in 2018 will be taught electronic evidence. Scary, is it not if you are a client?

Comments about Luddites and the move towards the use of digital technology – illustrating the clashes that have occurred – fail to indicate that it is not really about the introduction of technology, but the way society responds to those whose livelihoods are taken from them by the technology. As John Heathcoat discovered, the response to the loss of a livelihood could lead to violence and death of the inventor – he built a secret tunnel under his house at 38 Leicester Road in Loughborough, possibly as a means of eluding danger. It is doubtful that any software engineer has ever had to or will ever have to take such precautions.

The comments about autonomous cars are misguided (e.g 208). Not only does software code kill and injure people, but it has done so and will do so in autonomous motor vehicles. The deaths on the roads in motor vehicles in the UK are half that of France, a comparable country, as pointed out by the authors (289). The reason is simple: the French apply less attention to the safety of roads, do not enforce the use of seat belts and driver behaviour is dubious. Autonomous cars are not the answer. The motor vehicle industry are merely trying to invent unicorns. Note a letter by Professor Martyn Thomas, published in the *Financial Times* 1 October/2 October 2017:

> Sir,
>
> John Boothman (Letters, September 24) is unduly optimistic about driverless cars. Human drivers are remarkably safe: in 2013 in the UK there were 452 reported accidents for every billion miles driven and 85 per cent of these were not serious. These figures cover all types of roads in all weather conditions, day and night.

> To know that driverless cars are as safe as human drivers (to 50 per cent confidence) we would need evidence from more than 5m miles of driverless travel on the same mix of roads and the same distribution of weather conditions with zero accidents. Even then, when so much of the safety depends on computer logic, how will we show that thousands of cars are still safe after each software update? What happens when a whole fleet of cars is found to be vulnerable to cyber attack, and perhaps used to blockade a city?
>
> We are a long way from knowing that driverless cars will be a net benefit. We should take the time to plan how we want the future to be, not just suffer what a free market may deliver.
>
> Prof Martyn Thomas London SW8, UK

See also Roger Kemp, 'Autonomous vehicles – who will be liable for accidents?', 15 *Digital Evidence and Electronic Signature Law Review* (2018) 33 – 47.

On crime, as long as humans exist, crime will continue – because it is some humans define what a crime is – and other humans either do not agree or do not care. Crime will not be 'removed' (234).

The authors advocate that children should learn how to code – great, so they can write software for health devices that are capable of killing and injuring people. This is not a joke, as discussed in a recent event at the Royal College of Physicians in association with the University of Swansea: *Medicine, Machines and Healthcare Regulation: Is the Digital Agenda Safe and Effective?* (18 July 2018).

Personal data is indeed an issue (267-268), and a suggestion is that it becomes a right of the individual, but little has been done on this as yet, for which see Stephen Mason and Timothy S. Reiniger, '"Trust" Between Machines? Establishing Identity Between Humans and Software Code, or whether You Know it is a Dog, and if so, which Dog?', *Computer and Telecommunications Law Review*, 2015, Volume 21, Issue 5, 135 – 148.

This is an interesting read, but illustrates the need for an inter-disciplinary approach, and between people in disciplines that actually know what they are talking about.

Title: **Artificial Intelligence The Practical Legal Issues**

Author: **John Byers**

Date and place of publication: **United Kingdom, 2018**

Publisher: **Law Brief Publishing**

ISBN: Hardback **978 1 911035 82 4**

John Byers is a solicitor specializing in commercial law and leads the international artificial intelligence group at Osborne Clarke.

He has distilled into a short book the issues that arise when dealing with software code generally, as well as when it can be considered to be brought within the ambit of artificial intelligence – which is, essentially, the digital world in which we inhabit now. (Actually, it is algorithmic intelligence, although no publisher will change the title to be more accurate, for which see Stephen Mason, 'Artificial intelligence: Oh really? And why judges and lawyers are central to the way we live now – but they don't know it', *Computer and Telecommunications Law Review*, 2017, Volume 23, Issue 8, 213 – 225).

It would have been nice for the author to refer to robots as machines – which they are, and not to refer to software code as being a miracle (p 1) – especially when so many people have been killed and injured by software code, and not a software engineer or company held to account (for which see Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017), chapter 6).

In considering the deaths of people, the author refers to the Toyota unintended acceleration cases from the

United States of America (p 29) (these cases happen all over the world, but are not reported frequently). The *Bookout* case (*Electronic Evidence*, chapter 6) demonstrates that occasionally a judge will permit the claimant to view software code to help establish causation – a rare thing indeed – as judges seem to accept the arguments by software companies that because their code is proprietary and secret, it is not appropriate to give the other side a copy to analyse. So how do you determine causation? That is, if you do not know what the cause was, especially when dealing with the complexities of software code in motor vehicles (containing more lines of code than an aircraft). Simple the author indicates: by use of the principle *the thing speaks for itself*.

(Incidentally, the author makes a nice point by providing the translation, even though this text is written for lawyers. Even in the twenty-first century, judges and lawyers still like to use dead languages, such as Latin, and some think *res ipsa loquitur* is the correct way of expressing this term, which seems a little bit absurd, given it has to be translated into English, as the author has done. Latin has supposedly been banned by judges in European jurisdictions, for which see Stephen Mason, editor, *International Electronic Evidence* (British Institute of International and Comparative Law, 2008), xiii-xix).

The author cites a US case to support the argument that *the thing speaks for itself*: (2012) WL 5763178 (Texas). This reviewer has asked the author about this citation, because it seems to be incorrect. The actual citation that this refers to is a case from California, not Texas: *In re Toyota Motor Corp. unintended acceleration marketing, sales practices and products liability litigation*, 978 F.Supp.2d 1053 (C.D.Cal. 2013), 92 Fed. R. Evid. Serv. 714, Prod.Liab.Rep. (CCH) P 19, 244, 2013 WL 5763178. It was a hearing on sixteen motions to exclude expert testimony. Unfortunately, the author has not got back to the reviewer on this detail.

The author has made an important point about the legal concept of *the thing speaks for itself*. It is this: in the absence of the manufacturer providing the software code to help establish causation, then the only way a litigant can hope to achieve redress is for a judge to invoke this concept and find the manufacturer liable. Unfortunately, there does not seem to be any case where this legal concept has been used successfully. If this legal concept has been used effectively in relation to software code, the reviewer will be delighted to be informed.

Two little side issues arise:

> (i) At p 47 the author refers to the 'Rumsfeldian 'unknown knows''. This was first written about by D. H. Lawrence in his poem *New Heaven and Earth*:
>
> > 'now here was I, new-awakened, with my hand stretching out
> >
> > and touching the unknown, the real unknown, the unknown unknown'
>
> (ii) Also, footnote 15 (p 48) refers to 'keeping use of fata visible' – this seems to indicate a lack of proof reading – if not, just one of those errors, if it is an error, that creeps through, as all authors are only too well aware, although the liberal use of 'per se' is usually in italics, but not everywhere (p 55). There are other formatting issues, but that is a problem for the publisher.

It would be good to be given some examples the 'oft quoted popular fallacy which assumes infallibility and impartiality of such systems' (p 67) (apart from the ludicrous presumption that computers are reliable, for which see *Electronic Evidence*, chapter 6, upon which the author is silent).

Minor issues aside, this is a must-read book for anybody advising on aspects of software code if it is part of a device or product. The author beings his wide knowledge of the topic to bear in a text with few references, as the contents illustrate.

Chapter One – An Introduction to Artificially Intelligent Systems

Chapter Two – Causation and Artificial Intelligence

Chapter Three – Big Data and Artificial Intelligence

Chapter Four – Intellectual Property Rights in AI Systems

Chapter Five – Automated Bias and Discrimination

Chapter Six – AI Crime: Commission and Judgment

Chapter Seven – Market Distorting Effects: AI and Competition Law

Chapter Eight – Sector Specific Considerations

i. Lifesciences, Medicine & Healthcare

ii. Retail & Consumer

iii. Financial Services

iv. Transportation

v. Energy and Utilities

vi. Infrastructure and the Built Environment

Chapter Nine – Robotic Process Outsourcing and Artificial Intelligence as a Service (AiaaA)

Chapter Ten – Artificial Intelligence and Corporate Law

Chapter Eleven – Managing Machine Learning Systems on a Practical Basis

Title: **The Digital Estate**

Author: **Leigh Sagar**

Date and place of publication: **United Kingdom, 2018**

Publisher: **Sweet & Maxwell**

ISBN: **978 0 414 06190 3**

Leigh Sagar is a barrister whose practice includes the administration of digital information. He notes in the preface that he was first asked to advise on digital assets in 2014. The reviewer recalls this topic being discussed in 2005 at events, and realised that is was going to be an important issue. The author has brought out a timely text on the subject.

The text begins, in chapter 1, with the concepts that will permeate the topic – digital assets, digital records, digital information, and a basic introduction to how computers work. For more detail, see Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017), chapter 1, including the concept of trespass, for which see Ian Walden, *Computer Crimes and Digital Investigations* (2nd edn, Oxford University Press, 2016).

Chapter 2 deals with the fiduciary, data processing, personal representatives, trustees and attorneys and deputies, and puts into context the relevant duties and issues that affect the digital estate. To the uninitiated, the dangers of intermeddling are neatly noted at 2-28, and the problems of obtaining access to a cloud account are highlighted at 2-30, where the terms of use of a service provider are very important to read and digest respecting possible problems with authority to obtain access to a deceased persons digital assets: and 2-36 provides a list of excellent practical issues that may need to be addressed.

The chapter on electronic documents and electronic signatures provides a basic introduction to the uninitiated (see *Electronic Evidence*, chapter 3 for a detailed discussion of the foundations of evidence in electronic form, and Stephen Mason *Electronic Signatures in Law* (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016)) – the author does cite this text in passing (fn 20, 1-16 and the bibliography). The author provides a succinct outline of *J Pereira Fernandes SA v Mehta* [2006] EWHC 813 (Ch); [2006] 1 WLR 1543; [2006] 2 All ER 891; [2006] 1 All ER (Comm) 885; [2006] All ER (D) 264 (Apr); [2006] IP & T 546; (2006) The Times 16 May 18 (at 3-43 and 5-18). This is interesting for two reasons. First, the author has cited case law from other common law jurisdictions in the book to illustrate various important points, yet fails to consider decisions from other jurisdictions on whether the name in an e-mail address can be a form of electronic signature – a significant issue in this case.

Second, it will have been of interest for the author to have discussed the technical issues and conclusions of this case as considered in *Electronic Signatures in Law* at 11.29 – 11.39.

On metadata and logs in general, it must be emphasised that the metadata and other logs can only report on *purported* information such as the author, etc (3-07). To indicate that the metadata and logs are always accurate is misleading (for which see *Electronic Evidence*, 1.26, 2.22, 2.23, 2.26, 3.25, 5.24, 5.28). Many judges and lawyers fail to understand this important and highly significant point.

The discussion in chapter 4 on information as property is essential. The author takes the reader through the various discussions and decisions made by judges on the meaning of property and data in digital form, considering case law from England and Wales, the United States of America, Australia and New Zealand. This discussion is highly significant, given the number of records, statutory permissions and financial digital cryptographic tokens that might be at issue in the digital estate. At issue is whether digital data can be property. As the author indicates, judicial pronouncements are contradictory and hardly relevant to the world in which we live now (4-25 to 4-27).

The author notes the New York case of *Thyroff v Nationwide Mutual Insurance Company* 8 N.Y.3d 283, 864 N.E.2d 1272, 832 N.Y.S.2d 873 (the author gives a citation that predates publication in the Official Reports: 2007 NY Int. 29, at 4-42 fn 72) where an action for conversion relating to digital data held by a third party in the cloud. The question was whether the law applied to electronic computer records and data. Based on the facts of this case, the court held that the plaintiff did indeed maintained a conversion claim. The decision by Graffeo J in the Court of Appeals of New York (at 1278, internal citation omitted) reminds us that the law needs to remain relevant:

> 'In light of these considerations, we believe that the tort of conversion must keep pace with the contemporary realities of widespread computer use. We therefore answer the certified question in the affirmative and hold that the type of data that Nationwide allegedly took possession of—electronic records that were stored on a computer and were indistinguishable from printed documents—is subject to a claim of conversion in New York. Because this is the only type of intangible property at issue in this case, we do not consider whether any of the myriad other forms of virtual information should be protected by the tort.
>
> Accordingly, the certified question should be answered in the affirmative.'

The author compared this case to the decision in the English case of *Your Response ltd v Datateam Business Media Ltd* [2014] 3 WLR 887, [2014] CP Rep 31, [2015] QB 41, [2014] 4 All ER 928, [2014] EWCA Civ 281, [2014] 2 All ER (Comm) 899, [2015] 1 QB 41, [2014] WLR(D) 131 (set out at 4-21), where the members of the Court of Appeal rejected the idea that digital data could be information.

The decisions might be inconsistent, as pointed out by the author (4-43), but a judge in a New York court is not going to be concerned about a decision on the Court of Appeal in England (for which see Stephen Mason, 'Towards a global law of digital evidence? An exploratory essay', *Amicus Curiae* The Journal of the Society for Advanced Legal Studies, Issue 103, Autumn 2015, 19 – 28). The decision of Graffeo J is undoubtedly the better of the two, and reflects the fact that judicial decisions ought to be expansive and responsive to the changes in the world in which we live – which English judges have mentioned many times in the context of the meaning of a 'document', yet they fail to contribute to the development of the law in this arena. It is most strange. In response, Fullerton J of the New South Wales Supreme Court in the case of *Gammasonics Institute for Medical Research Pty Ltd v Comrad Medical Sysytems Pty Ltd* [2010] NSWSC 267 suggests a change in the law was more appropriate (at [42] and [43]), as noted by the author at 4-48.

Regardless of whether judges exercise their powers or Parliament takes the initiative, change is overdue in changing the sorry state of affairs as described by the author in this text, for which see 4-69.

As a side comment, in discussing financial digital cryptographic tokens, the author raises a smile in his description of the imaginary tea party at 4-88. Recommended reading.

In general terms, the author raises a broad point of significance regarding the terms and conditions of services offered by a range of cloud providers and social media sites, to name but two examples – by which it is noted that the terms and conditions can act to prohibit apparently quite normal actions relating to physical items, but fails in the digital environment – where the terms are such that if anybody other than the customer obtains access to an account, they are breaching the agreement (8-04). The reaction to this by United States and Canada is helpful, and it will be interesting to know if this important issue is on the political agenda in the UK – perhaps it will be after a patrician politician is on the wrong end of such draconian terms.

By way of observation, it is interesting to note that another lawyer, Louise Lewis, possibly the senior associate of Penningtons Manches LLP, read the text – yet it appears that the author has not requested appropriately qualified technicians to peer review the descriptions of how a computer works, the internet or the description of digital signatures. Two independent people looked at a sample of the technical descriptions of digital signatures at 3-28 and 3-29 for the purpose of this report. One was Richard Trevorah, Technical Director of tScheme Limited (tScheme was the national body responsible for accreditation and supervision referred to in Article 3(4) of the EU electronic signature Directive, now repealed), and Alan Liddle, one of the founders and directors of Trustis Limited before his retirement. Richard and Alan both have extensive experience of advising on and installing digital signature schemes. A number of comments were made regarding the use of technical words that have precise meanings, for instance:

Page 56, item (b)(iv) reads 'the insertion of a sequence of numbers and letters that result from the encryption of a name or some other text'

Suggested change:

> 'the insertion of a sequence of numbers and letters that result from the encryption, based on a key known only to the signatory, of a name or some other text'

3-29(2) reads 'Alice's computer is able to run on software that has the use of two "keys", each of which is a long number.'

Suggested change:

> Alice's computer is able to run on software that has the use of two "keys". Depending on the algorithm chosen, the key is usually 1 or 2 separate numbers.'

Page 57(4), the text reads 'Alice's software then encrypts the message digest with her private key'

Suggested change:

> Alice's software then applies an algorithm to the message digest with her private key'
>
> [Using RSA she actually decrypts the digest to produce the digital signature, and with other algorithms it is neither.]

Page 57(ii) under Digital certificates, the text reads in part:

> 'Carol could alter Alice's message and hash the altered message to create a new, fake, message digest. She could then create a new, fake, private and public key set, in Alice's name, impersonate Alice and send the fake public key to Bob; use the fake private key to encrypt the altered message digest and then send the resulting

fake digital signature and altered message to Bob. Bob would use the fake public key (thinking it was Alice's true public key) to decrypt the fake digital signature and compare the result with the fake message digest; the two would be identical so that Bob would have been deceived into thinking that the altered message was the one that Alice sent.'

Comment:

The correct sequence is:

1) create false key pair;

2) use signature algorithm on digest to create digital signature;

3) impersonate Alice and send altered message, counterfeit public key and related digital signature;

4) Bob applies verification algorithm to altered message and related digital signature using forged public key and apparently gets a successful verification that message was from Alice.

Minor quibbles aside, in essence, the technical reviewers of this short piece of text concluded that it appears to be a very similar (but not exact) description used in support of the original RSA patent.

There is a puzzling inconsistency. It is traditional for the authors of legal text books to mention, as a matter of courtesy, relevant books on specialist topics in footnotes before providing a summary of the law. The author does this on some occasions (1-10 fn 9; 2-01 fn 1; 2-47 fn 134; 6-01 fn 1 and fn 2; 8-01 fn 1) but not others. No doubt this possibly inadvertent omission will be remedied in the second edition.

Finally, the suggested examples for drafting to take into account the digital estate in chapter 8 should prove to be helpful to practicing lawyers in this field. It will be interesting to establish quite how many practitioners become aware of this text, and if they do, whether they will obtain a copy and put it into practice. To date, few lawyers and judges seem that well aware of the central issues concerned with this journal. It is to be hoped that this will – eventually – change for the good of the clients they serve.

Contents

Title: **The Law of Driverless Cars An Introduction**

Author: **Alex Glassbrook**

Date and place of publication: **United Kingdom, 2017**

Publisher: **Law Brief Publishing**

ISBN: **978 1 911035 28 2**

Alex Glassbrook is a barrister whose practice includes cases involving road vehicles, driverless technologies, and high-value personal injury claims.

The author has set out the basic issues that arise when discussing motor vehicles that are controlled by software code written by human beings. He has divided the book into three: (i) the changing landscape, looking at the current position, (ii) the near future, in which he discusses personal data, accidents, crime, roads and insurance, and (iii) the future, speculating (of necessity) about personal data, risks and insurance and the road system.

This topic is in a constant state of flux, and the author might agree that his text is already a historical curiosity. Notwithstanding that some of the text is

rightly speculative, it illustrates some of the issues that will arise with motor vehicles being purchased at the time this Report is published, as much as an indication of things to come in the future.

Of interest are some of the issues that are not touched upon.

For instance, when an accident occurs, the significant problem of the legal presumption that computers are 'reliable' is not mentioned (for which see Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017), chapter 6) – this is important, taking into account the *Bookout* case in the United States of America, which is not mentioned by the author. Given the list of examples (in chapter 6 of *Electronic Evidence*) by which people have been killed and injured by software code over the years, the suggestion by the author (p 32) that 'fully driverless car should be reliable – if not perfectly so, then to a very high standard indeed (as close to unattainable 100% as could be realistically expected)' is a gross misunderstanding of the poor quality of software code written by humans for motor vehicles. This reviewer predicts that software code in motor vehicles will continue to kill and injure substantial numbers of people in the future.

The unintended acceleration cases illustrate another highly significant problem not mentioned by the author – that is, trying to persuade a judge to disclose software code to help determine causation (the *Bookout* case appears to be the only case thus far where a judge has resisted the blandishments of the motor manufacturers and their arguments of confidentiality and trade secrets). That difficulties with proving causation can happen to a family in which people were killed and injured because a motor vehicle that was far from being autonomous, serves to illustrate the problems that people will have in the future, unless manufacturers are the subject of strict liability.

Comments about the difficulties of proof are important (p 48), and it will have been of interest if the author had addressed this issue in more detail, taking into account the ridiculous presumption that computers are reliable (and by implication software code in motor vehicles is reliable – whatever that means – for an explanation, see the vignette 'Business Records' in *Electronic Evidence*, xii – xiii) and the highly significant fact that there is a lack of relevant expertise in this area. For instance, Kaushal Gandhi was tragically killed when his motor car crashed into a stationary vehicle on 2 February 2016. It appears that his Skoda Octavia motor car increased its speed and took over control of the vehicle from the driver. The Coroner recorded a narrative verdict. It is debatable whether the facts surrounding this case were adequately investigated. For media reports, see: 'Driver's last moments recorded in 999 call as he tells operator car's cruise control 'stuck' at 119mph', *The Telegraph*, 24 November 2016; Chris Johnston, 'Skoda driver decapitated after claiming car's cruise control was stuck', *The Guardian*, 24 November 2016; Shebab Khan, 'Driver decapitated in 119 mph crash after car 'got stuck in cruise control'', *The Independent*, 25 November 2016.

The author comments that the use of motor vehicles will change, as will models of ownership, which might be right. However, to suggest that cars for hire will be more accessible (p 33; p 39) is fanciful outside cities, as anybody living in the countryside will be aware – already people living in the country are subsidising city dwellers as banks continue to close down outside big conurbations.

The author mentions the possibility of an employee undertaking work as they travel in a motor vehicle controlled by software code (e.g. p 89), yet nowhere mentions the highly significant problem that it is easy to lose focus, and difficult to get it back. The author fails to discuss the liability of the employer if they require an employee to work in a motor vehicle controlled by software code. Getting a distracted driver to understand what is happening and to react in seconds is impossible. A great deal of work has been done on this, for which see a recent paper: S. Shen and D. M. Neyens, 'Assessing drivers' response during automated driver support system failures with

non-driving tasks', *Journal of Safety Research*, (2017) 61:149-155 – for an earlier example, see Will Knight, 'Driverless Cars Are Further Away Than You Think', *MIT Technology Review*, 22 October 2013. The death of Joshua Brown, travelling in a 2015 Tesla Model S 70D car illustrates the problem. The National Transportation Safety Board determined that the probable cause of the crash:

> 'was the truck driver's failure to yield the right of way to the car, combined with the car driver's inattention due to overreliance on vehicle automation, which resulted in the car driver's lack of reaction to the presence of the truck. Contributing to the car driver's overreliance on the vehicle automation was its operational design, which permitted his prolonged disengagement from the driving task and his use of the automation in ways inconsistent with guidance and warnings from the manufacturer.' (*Collision Between a Car Operating With Automated Vehicle Control Systems and a Tractor-Semitrailer Truck Near Williston, Florida May 7, 2016* Accident Report (NTSB/HAR-17/02; PB2017-102600), vi.

The author also asserts, as do many others (e.g. p 4, p 40), that motor vehicles driven by software code are safer than vehicles driven by humans. As noted in another Book Report in this issue (*The Digital Ape how to live (in peace) with smart machines* by Nigel Shadbolt and Roger Hampson), this is far from reality. There are other factors that can improve safety, and the United Kingdom has been successful in reducing fatal accidents significantly without recourse to vehicles controlled by software code.

There are indications that the text has not been proof read as thoroughly as one would like (a problem all authors are only too well of), but the errors appear to be few: p 33 'the need retain'; p 100 text is struck through.

This is a book that puts a number of relevant legal issues into one place by a practitioner. If a second edition is contemplated, it will be important to include some of the practical issues of proof noted in this review.