Title: **Electronic Evidence**

Editors: **Stephen Mason and Daniel Seng**

Edition: **Fourth**

Date and place of publication: **2017, London**

Publisher: **Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London**

ISBN: **978-1-911507-05-5** (hardback edition); **978-1-911507-09-3** (paperback edition); **78-1-911507-08-6** (epub version); ISBN **978-1-911507-06-2** (Kindle version); ISBN **978-1-911507-07-9** (Open Access PDF)

In this updated edition of the well-established practitioner text, Stephen Mason and Daniel Seng have brought together a team of experts in the field to provide an exhaustive treatment of electronic evidence. This fourth edition continues to follow the tradition in English evidence text books by basing the text on the law of England and Wales, with appropriate citations of relevant case law and legislation from other jurisdictions.

Contents

Title: **The Sciences of the Artificial**

Author: **Herbert A. Simon**

Edition: **Third**

Date and place of publication: **1996, Cambridge Massachusetts and London**

Publisher: **The MIT Press**

ISBN: Paperback **9780262691918**

In finding out what the late Professor Simon achieved with *The Sciences of the Artificial*, the following comment by Professor George A. Miller (*Complex Information Processing*) appears regularly over the internet:

> 'People sometimes ask me what they should read to find out about artificial intelligence. Herbert Simon's book *The Sciences of the Artificial* is always on the list I give them. Every page issues a challenge to conventional thinking, and the layman who digests it well will certainly understand what the field of artificial intelligence hopes to accomplish. I recommend it in the same spirit that I recommend Freud to people who ask about psychoanalysis, or Piaget to those who ask about child psychology: if you want to learn about a subject, start by reading its founding fathers.'

The description on the back cover of the present edition is also of interest:

> 'The natural sciences describe "natural" objects and phenomena. The sciences of the artificial describe objects and phenomena – artifacts – that result from human intervention in the natural world. Much of our daily world is artificial – from the climate-controlled air we breathe to the automobiles we drive and the laws that tell us how fast we may drive them. Aimed at satisfying human purposes, artifacts are not exempt from natural law but are adapted to the environments in which they operate.'

Herbert Simon was awarded, amongst others, the Turing Award in 1975 and a Nobel Memorial Prize in Economics in 1978, and this book considers some of the fundamental issues of the artificial without offering prescriptive advice to computer science or any of the other disciplines discussed as part of the thesis.

Humans have made the world in which we live. We live in a collective artifice, and Herbert set out what he thought the boundaries for sciences of the artificial might be (p 4):

> '1. Artificial things are synthesized (though not always or usually with full forethought) by human beings.
>
> 2. Artificial things may imitate appearances in natural things while lacking, in one or many respects, the reality of the latter.
>
> 3. Artificial things can be characterized in terms of functions, goals, adaptation.
>
> 4. Artificial things are often discussed, particularly when they are being designed, in terms of imperatives as well as descriptives.'

The question is how to build a reliable system from unreliable parts. Herbert might not have considered this precise question in relation to software code, but he explained the issue very clearly in the context of humans from organizations:

> 'As creatures of bounded rationality, incapable of dealing with the world in all of its complexity, we form a simplified picture of the world, viewing it from our particular organizational vantage point and our organization's interests and goals.'

This is what has occurred in the legal world in relating to software code in machines. There has been a collective failure to understand that, to achieve any form of justice, causation cannot be determined by ignoring the black box of software code. The software code must be revealed. In this respect, Herbert considers the difference between the inner and outer environments, as described by using the aeroplane as an example (pp 6 – 7):

> 'A theory of the airplane draws on natural science for an explanation of its inner environment (the power plant, for example), its outer environment (the character of the atmosphere at different altitudes), and the relation between its inner and outer environments (the movement of an air foil through a gas).'

Herbert goes on to explain about the human and how we think (p 53):

> 'A thinking human being is an adaptive system; men's goals define the interface between their inner and outer environments, including in the latter their memory stores. To the extent that they are effectively adaptive, their behavior will reflect characteristics largely of the outer environment (in the light of their goals) and will reveal only a few limiting properties of the inner environment of the physiological machinery that enables a person to think.'

The problem is, that the participants in the legal system mainly think and respond to the outer environment in the light of the system in which they operate, which in turn is highly simplistic when concerning machines operated by software code, which highlights Herbert's conclusion (p 110) that 'Human beings, viewed as behaving systems, are quite simple.'

It is important for participants in the legal system (including legal academics) that they must begin to understand the sheer complexity of the world in which we operate, including the weaknesses of software code. Herbert commented (p 251) that:

> 'How complex or simple a structure is depends critically upon the way in which we describe it. Most of the complex structures found in the world are enormously redundant, and we can use this redundancy to simplify their description.'

In England & Wales, the Law Commission decided, in 1997, to have a legal presumption that computers were 'reliable' (this is short-hand for what was determined, and a detailed discussion can be found in chapter 6 of Stephen Mason and Daniel Seng, eds, *Electronic Evidence* (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017). No judge has ever set out what 'reliable' means in relation to machines operated by software code, yet every day in both criminal and civil proceedings, this presumption applies – and a similar assumption applies in other common law jurisdictions. The lawyers have decided to describe computers is a simplistic way, and in so doing, have made the way they work redundant. This might be a convenient method of dealing with complex systems, but does not help in working towards justice in the age of the connected digital device.

Although this book is not specifically directed to lawyers, nevertheless it is a reminder of the complexities of the world in which humans have constructed, and as such ought to act as a reminder that complexity is normal and should be acknowledged by the law.

Contents

Title: **Spreadsheet Check and Control: 47 key practices to detect and prevent errors**

Author: **Patrick O'Beirne**

Date and place of publication: **2005, United Kingdom**

Publisher: **System Publishing**

ISBN: **190540400X**

Lawyers often think they do not need to know anything about software code in machines. They ought to think again, and this book will illustrate why – for lawyers use spreadsheets in their own practice, but are also required to provide appropriate legal guidance to clients when the accuracy of spreadsheets are in question.

Although this book accompanies a course on spreadsheets (the Advanced Course of the European Computer Driving License (ECDL)), the lessons clearly illustrate the complexity of spreadsheets and how to avoid mistakes. The author is Chair of the European Spreadsheet Risk Interest Group Management Committee, a group that has been going for some time, as explained on the web site (http://www.eusprig.org/):

> EuSpRIG was founded in March 1999 as a collaboration between spreadsheet researchers at the University of Greenwich, the University of Wales Institute Cardiff and HM Customs & Excise. Its mission was to bring together academics, professional bodies and industry practitioners throughout Europe to address the ever-increasing problem of spreadsheet integrity. EuSpRIG was founded by Pat Cleary (UWIC), David Chadwick (Univ. Greenwich) and Ray Butler (HMRC). They were first introduced to each other by Professor Ray Panko (University of Hawai'i).

The fact is, spreadsheets contain errors, and the EuSpRIG web site has a page illustrating public reports of spreadsheet errors that Patrick has been accumulating over the years. Some are minor, but the more serious include errors of omission and errors of logic, where the model or calculation is incorrect. The problem is exacerbated because the code and data are mixed, which means it is not easy to deal with the complexity of spreadsheets.

The marketing material provides a useful and accurate summary of the text:

> The process of design, specification techniques, the use of appropriate documentation, security, backup, protection, and the development of conventions, formats and internal corporate standards.
>
> Shows how to check for unusual settings, for example with rounding and precision, which are the source of traps for the unwary.
>
> How to identify the causes of error values, methods of error handling, and how to detect missing inputs and calculations.
>
> It explains how:
>
>> (i) common mistakes arise when structural changes are made, and common problems with known error-prone formulas and external links;
>>
>> (ii) to discover inconsistencies and mistakes, correct them, recover from incorrect operations, and create self-checking formulas.

The display section shows how to uncover hidden and obscured data and formatting, how to discover problems with data types, and incorrect sorting and queries in database ranges.

The use and abuse of charts is illustrated.

Spreadsheet testing and review, including how to:

(i) create and run test cases

(ii) build in cross-checks for internal control

Auditing techniques are also described, such as how to reveal hidden formulas, rows, columns, worksheets, and data integrity and validation are also described.

In summary, this is a useful book to have on the shelf. It will be of great help to the lawyer trying to make sense of spreadsheet evidence prior to asking an expert witness to offer a more in-depth explanation of the evidence in a particular case.

Title: **The Future of Law and eTechnologies**

Editors: **Tanel Kerikmäe and Addi Rull**

Date and place of publication: **2016, Switzerland**

Publisher: **Springer International Publishing**

ISBN: Hardback: **978 3 319 26894 1**; eBook **978 3 319 26896 5**

The marketing blurb on the cover of this book suggests it is 'groundbreaking' – for this reader it was interesting and highly recommended to law students in particular, but the value is mainly in the claim that it will provide a source for interdisciplinary research – which is very much needed across the law and information technology. In this respect, this text will be a useful addition to every law library.

The introductory essay *Theorising on Digital Legal (Outer)Space* by Professor Tanel Kerikmäe and Addi Rull considers how laws are developed in the European Union. First, it is to be noted that legislation is increasingly shaped by the monopolist commercial entities, especially from the United States of America, who spend significant sums of money on lobbying politicians and regulators – yet ordinary people are rarely aware of this elephant in the room – for which see the comments by John Lancaster in 'You Are the Product' for one aspect of how technologists control life today (*London Review of Books*, Volume 39, Number 26, 17 August 2017, 3 – 10, available online at https://www.lrb.co.uk/v39/n16/john-lanchester/you-are-the-product). How is this stranglehold to be ameliorated? How do we ensure legislation is not passed to favour the commercial behemoths?

Second, the authors rhetorically state that 'New technologies are making us smarter' (p 1). This is a highly significant assertion that has shaped this review, as it shaped the content of this book.

Considering the law in relation to contract terms, no legal system permits consumers to challenge contract terms effectively – yes, they can read through all 30 or 100 pages if they want to and try to understand the legalese employed in many jurisdictions, but they cannot negotiate out terms they do not wish to remove before entering a contract – so why read the terms? It is perfectly rational, if one wants to use software, for instance, to accept the terms without reading them – for if you read them and decline to accept one or two terms that you consider to be unfair, you do not have the option of removing them from the contract. A consumer, at best, can take expensive and lengthy legal action to have a contract term declared unfair. But so what? Why does the law permit the use of contract terms that must be accepted? How does technology make this smarter? In the age of information technology, the legal rules gives an even better advantage to the commercial entity, leading inexorably to the control of personal data that is now the norm, and has, incidentally, significant ramifications to the discussion by Kaido Künnapas in *From Bitcoin to Smart Contracts: Legal Revolution or Evolution from the Perspective of de lege ferenda?*, who point out that crypto currencies share the characteristics of fiat money, and set out the legal gray areas, especially because such 'currencies' tend not to be controlled by legal entities, which means applying legal rules is problematic (for a brief history, see Arvind Narayanan and Jeremy Clark, 'Bitcoins Academic Pedigree The concept of cryptocurrencies is built from forgotten ideas in research literature', *acmqueue*, Volume 15, Issue 4, August 2017, https://queue.acm.org/detail.cfm?id=3136559). In *Smart Contracts*, Merit Kõlvart, Margus Poola, and Addi Rull conclude that automated contracting can fulfill certain tasks, but make it clear to the technicians that promote 'smart contracts' that such terms will always be subject to normal contract law. Maria Claudia Solarte-Vasquez, Natalia Järv, and Katrin Nyman-Metcalf consider practical issues in *Usability Factors in Transactional Design and Smart Contracting*, including the use of arcane language that is used by lawyers when preparing contracts, which is unnecessary. Most lawyers in England and Wales have moved away from such ridiculous practices, partly because of the penalties imposed by judges over the decades and partly because clients want plain language to be used.

Third, Alexander Norta, Katrin Nyman-Metcalf, Anis Ben Othman, and Addi Rull consider one issue in *"My Agent Will Not Let Me Talk to the General": Software Agents as a Tool Against Internet Scams*, suggesting that software code might be able to help people stop falling for scams – yet they conclude that such 'intelligent' agents will probably, if developed, be used by people with a good awareness of life generally and have a suspicion about something that is too good to be true (pp 42 – 43). Regardless of technology, the most vulnerable remain the most vulnerable.

Of the other chapters in this interesting text, Professor Lehte Roots and Costica Dumbrava consider *E-Citizenship Opportunities in the Changing Technological Environment*, and Sandra Särav and Professor Tanel Kerikmäe consider the Estonian e-residency project in *E-Residency: A Cyberdream Embodied in a Digital Identity Card?*. Electronic citizenship seems to be somewhat of a arcane concept, given that we exist as physical biological animals that have a significant sized brain, and have used our ability to communicate and cooperate to dominate the planet to the detriment of all other life forms. Humans have created technology, but technology should not be used as yet another method of control – although that is precisely what commercial entities and politicians are using it for. Sandra Särav and Professor Tanel Kerikmäe illustrate the inconsistencies of the political aims and practicalities of the Estonian e-residency scheme, which can be described as a cute and amusing little project. Kristi Joamets also considers the legal control of marital relationships between people in the chapter *Digital Marriage and Divorce: Legality Versus Digital Solutions*, concluding that it is doubtful that digital marriage will encourage people to marry, although the author points out (p 191) that children are increasingly born outside wedlock. Even if it is possible to overcome the legal obstacles, once has to ask why a physical act between two people living in the physical world should be available in the digital world. The technologists might develop something because they can, but 'because' is no reason for substituting the digital world with the physical when regulating human relations.

The problems of controlling intellectual property, as every musician, writer and film maker is only too well aware, is considered by Paula-Mai Sepp, Anton Vedeshin, and Pawan Dutt in their chapter in relation to 3-D printers: *Intellectual Property Protection of 3D Printing Using Secured Streaming*. Possible legal and technical solutions are considered, noting that the complexity of 3-D printing is such that the current laws relating to copyright do not cover the entire process.

Finally, Agnes Kasper and Eneli Laurits carried out an analysis of the literature available on one electronic database – EBSCO – to identify the main scientific contributions and legal problem areas relating to collecting evidence in digital form (p 198). Naturally, this left out a considerable body of relevant articles and books in their chapter *Challenges in Collecting Digital Evidence: A Legal Perspective*. Both have practical experience in this area, and concentrate on illustrating how useful it will be for organizations, both commercial and non-commercial, to ensure IT systems are designed to support the need to adduce digital data as evidence in legal proceedings. Interestingly, the authors discuss the differences between civil law and common law systems, citing the Latin tag *nemo tenetur edere instrumenta contra se* principle (p 204). This is a rule from ancient Roman Law, meaning no one is bound to produce instruments against himself – a rule that remains in criminal law. The authors note that this rule has been gradually abandoned in the interests of justice (about time, many litigants will say) in some jurisdictions, but many lawyers in continental Europe express incredulity when they discover the English civil procedure rule set out in Part 31, which reads:

> 31.6 Standard disclosure requires a party to disclose only–
>
> (a) the documents on which he relies; and
>
> (b) the documents which –
>
> > (i) adversely affect his own case;
> >
> > (ii) adversely affect another party's

case; or

(iii) support another party's case; and

(c) the documents which he is required to disclose by a relevant practice direction.

For some reason best known to them, continental lawyers seem to think that legal proceedings are perfectly fair if the parties do not have to produce all the relevant evidence in civil legal proceedings – a strange doctrine that used to be the norm in England and Wales until jurists saw the light. Perhaps our continental colleagues will follow the lead eventually – after all, one does not have to follow the rules laid down in ancient Rome under different material circumstances. The purpose of the system of justice is to aim to establish truth, and in so doing, fairness between the parties. How can this be achieved if all the facts are not available to the adjudicator?

In summary this text is highly recommended – it sparks questions, which a good book should do.

Title: **Programmed Inequality How Britain Discarded Women Technologists and Lost Its Edge in Computing**

Author: **Marie Hicks**

Date and place of publication: **2017, Cambridge, Massachusetts**

Publisher: **The MIT Press**

ISBN: Hardback **978 0 262 03554 5**; eBook **978 0 262 34292 6**

Professor Hicks has written a very interesting and depressing book about the appalling way in which successive governments in the UK treated women, so much so that there is no question that the development of the UK computer industry suffered significantly as a result, including the problems successive governments had regarding the problems of operating computers. It is not always the case that it takes an outsider to see the faults of the native, but this text is similar to the ground breaking work of Samuel Pyeatt Menefee, and who took a DLitt at Oxford University, finding a publisher for his thesis in 1981, *Wives for Sale* (Basil Blackwell, Oxford). The difference between these books is that a UK publisher published his text, whereas a US publisher published this book by Professor Hicks, and it shows (more of that later).

Professor Hicks makes it clear that without women, the work at Bletchley Park would never have achieved the results it did during the war, and after the war women in computing were considered to be valuable – in fact so valuable, that the mandarins (from public schools and the best UK universities, so well educated) in the Civil Service gave them a new rung on the Civil Service ladder – machinists – that is, a new grade, the lowest of the low, and at the same time, forbid women to be promoted above this grade. As the years progressed and it became even more important for the government to utilise computers in a variety of work, so the elite male Civil Servants and Ministers of government agreed that a new hierarchy had to be established to permit *men* to have a career with computers. Because men had no knowledge or experience of these complex machines, nor knew how to run or write programs or manage them, women at the top of the machine grade were required to train newcomers for up to a year, so that the male newcomer could then take over and enter a new managerial role and in turn become the manager of the trainer.

Not only were women humiliated by 'educated' men from the 1940s to the 1980s in this way, but they were also prevented from being paid a salary commensurate with the expert knowledge they had to have, and attempts to ask for higher pay were usually met with re-grading in such a way as to ensure they remained on low wages – even after the UK ratified the Universal Declaration of Human Rights (proclaimed by the United Nations General Assembly in Paris on 10 December 1948, at the 183rd Plenary Meeting of the General Assembly, resolution 217A) – which meant the UK eventually implemented the provisions of article 23 across government. It took until the UK joined the embryonic EU to implement equal pay for women, and then only after being forced to do so and in a way that meant women had to undertake years of litigation before their position was adequately dealt with my business.

The rational rested on three false assumptions (pp 1 – 2):

(i) Computers were women's work, as the war years established – demonstrating how simple the work was, and once the content of the work appeared to alter with technological changes, so males were introduced, which led to the reverse assumption: that because computers were now complicated, men needed to take over.

(ii) The control of machinery was usually a woman's job, but once computers became wholly electronic, men had to be in control.

(iii) Women left the field because of a lack of interest, lack of relevant skills, or they were just not good enough to play a major role (nothing to do with having to leave employment if you got married – a bar that continued unofficially for many years after it was abolished – and that there was no opportunity to progress and make a career).

This is all stuff and nonsense, as Professor Hicks illustrates.

Furthermore, the fact that women were the mainstay of computers and computing in the public service continues to be overlooked, as Professor Hicks points out (p 43) in citing the Science Museum's exhibit in 2012 on wartime code breaking, a description read that 'machines operated around the clock' without telling the reader that the machines were all operated around the clock by women. This is similar to the description of the introduction of containers into world shipping by the Design Museum in London (the panel was viewed by the author in August 2017), in which it was stated that containers improved trade (which they did) and, with a photograph of a ship being unloaded by hand prior to the use of containers, the text continued to indicate that before containers, loading and unloading ships was 'chaotic' – as if humans had been loading and unloading ships in a state of chaos for thousands of years, never mind that men knew what they were doing, from the legal rules and documents to people creating and controlling the paper work to those doing the physical work. Robin Law Fox has cause to complain of similar inaccuracies, in 'A matter of National Trust', *Financial Times*, *House & Home*, 16 September/17 September 2017, 24. So much for 'education' – as His Holiness the XIVth Dalai Lama wrote in *The Paradox Of Our Age*, 'We have more degrees, but less sense'.

On equal pay, Professor Hicks slips in a discussion about sexuality and how the police hounded homosexual men (p 60). Keith Dockray and Alan Sutton, *Politics, Society and Homosexuality in Post-War Britain: The Sexual Offences Act of 1967 and its Significance* **(**Fonthill Media, 2017) highlight the points made by Professor Hicks that the appointment of Sir Theobald Mathew as Director of Public Prosecutions in 1944 lead to an increase in the prosecution of homosexual men, and he was supported by Herbert Morrison when he became Home Secretary. However, the pressure to increase prosecutions in the United Kingdom came from the United States, and the later conservative Home Secretary, Sir Davis Maxwell-Fyfe, escalated prosecutions. (See also Lucy Delap, 'Campaigning for homosexual rights in 20th-century Britain' in *Campaigning for change: Lessons from History* (Friends of the Earth), individual chapters available at https://www.foe.co.uk/blog/campaigning-change-can-we-learn-from-history).

Austerity was also an excuse to keep wages down, and Professor Hicks reminds us of the London smog of 1952 (p 63), noting that some witnesses saw policemen lead busses through London streets with flashlights – and my father-in-law, Eddie Rosser, tells us of the time when he and his chums, at 15, used to make up flares on wooden sticks using rags and oil, and would go into Richmond (SW London) town centre to offer to guide the bus driver as far as Kew Bridge without asking for payment – for fun, returning to Richmond for another bus. Unwittingly, adding to the pollution.

This book is a must-read for anybody that has anything to do with computing in the UK in particular, because the UK would not necessarily be the 'second-rate' nation it apparently is now if the role of women had been properly recognized. (Professor Hicks describes the UK as 'second-rate' on a number of occasions, without defining what she means by 'second-rate' – maybe the UK is 'second-rate' because it was only rated 5th in the world ranking for GDP in 2016 by the World Bank? It is like the comment by Professor John G. Gallaher in his text *General Alexandre Dumas Soldier or the French Revolution* (Southern Illinois University Press, 1997) that the future general 'undoubtedly underwent the customary hazing [meaning undergoing an initiation ceremony] of all new recruits' (p 14) – intimating, in the absence of any historical facts, that the French army in the eighteenth century had the same attitude to embarrassing and humiliating people as the Americans).

A trifling consideration is the assumption that marketing by British companies engendered British cultural and imperial *supremacy* (pp 117 – 121). This is somewhat confusing, given that the British influence in India was poor after India became a country for the first time in history, for which see V. G. Kiernan, *America The New Imperialism From White Settlement to World Hegemony* (2005), p 305. Professor Hicks cites Edward Said, *Orientalism* (1978) in support of the assertion of British cultural hegemony, failing to indicate that a great deal of criticism was levelled against this book, although it was undoubtedly influential. Consideration was rightly given to the financial support of the British commercial computer industry by successive British governments, and there Professor Hicks has included one reference acknowledging that the taxpayer in the United States provided even greater financial support to IBM in the same way that 'socialist' countries support their industries (chapter 5, footnote 3).

A minor blemish is the failure to remove colloquial language. This is a failing of many US publishers that intend their books to be bought outside the United States. The author uses a number of unintelligible terms: 'boondoggle' (p 65), 'roiled' (p 70), 'cheesecake' (p 116), 'metrics' (p 132) – meaning measurements?, and 'slated' (p 207). Bearing in mind the topic of the text and the likelihood that most of the copies will be purchased in the United Kingdom, it demonstrates, perhaps, a certain cultural imperialism, and a failure on the part of the editors to notice and replace these colloquial terms.

Minor blemishes aside, the discussion at pp 221 – 224 is first rate, and encapsulates the problems faced by women and computing in the UK. This is a must-read. For this reason, I dedicate this book report to my mother-in-law, Mary, who was one of those early 'computers' or 'machinists' that worked variously for the British Electricity Divisional Authority at Kingston, the Mercantile Credit Company in the West End of London with offices behind Oxford Circus, and other commercial companies in Twickenham at the beginning of her working life in the 1950s, and knew what it was like to deal with Hollerith cards every day, together with the noise, as noted by Professor Hicks (p 209). It was fascinating going around the National Museum of Computing with her.

Professor Hicks is to be thanks for writing an interesting and valuable book about an important part of British history, reminding us of the struggle women have had in the past – and continue to have in the present.

Contents

Title: **Weapons of Math Destruction How Big Data Increases Inequality and Threatens Democracy**

Author: **Cathy O'Neil**

Date and place of publication: **2016, 2017, United States of America**

Publisher: **Broadway Books, imprint of Crown Publishing Group, division of Penguin Random House LLC**

ISBN: **978 0 553 41883 5** (version provided by the publisher); eBook **978 0 553 41882 8**; international edition **978 0 451 49733 8**

Politicians ought to read this book by Cathy O'Neil. Then, just maybe, they might be convinced that the right thing to do in the world in which we live now is to stop listening to software companies and start changing the law to take into account the disastrous world in which we now live. Also, journalists in the media ought to read it as well, and then, maybe, just maybe, they might start reporting on the industry in a more balanced way. Some hope. Many people already know what it is like to be at the wrong end of decisions made by software code, and the numbers affected will increase as commercial entities and governments fall for the hype hawked by the software industry year after year.

Cathy O'Neil is a mathematician and data scientist, and has illustrated the maladjusted world in which we live now – based, as the author points out, on software applications that in turn are written by human beings (mostly men), with choices as to how the software code is written, on the basis of prejudice, misunderstanding and bias (p 3), resulting in software code that is opaque. Software writers define their own reality and then use it to justify the results. At present, the significant distinction is between the privileged, who are generally not scored detrimentally by software code, and the poor, who are.

In writing software code, programmers routinely lack data for human behaviour, which means they substitute data from dubious statistical correlations that discriminate and are even illegal to use (pp 17 – 18). The author uses an example from the schools in Washington D.C. to demonstrate the simplicity of the models used to determine whether a teacher is competent, pointing out that software code is like racism, in that it is haphazard, includes spurious correlations, reinforces inequalities and confirms bias (p 23). This is illustrated (chapter 2) by the author via her own experience and the software code used by the credit-rating agencies in the lead up to the crash of 2007 (a complimentary analysis of the problems is set out in the open source practitioner textbook Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th end, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London), 6.131 – 6.136). There were two false assumptions in operation regarding the run up to the banking fiasco: the algorithms devised by the mathematicians were used to carefully balance risk, when the purpose of the software code was to provide the best short-term profits for sellers, and second, it was assumed that not many people would default at the same time. The author was forced, in her own words, ‘to confront the ugly truth: people had deliberately wielded formulas to impress rather than clarify’ (p 44). This highlights a significant concern that seems to be ignored: it is important to know the objectives of the modeler to understand how to tackle the decision-making process of software code.

Cathy O’Neil uses a number of examples (including targeting voters in elections, education, the justice system, for profit universities, credit scoring) to demonstrate the dramatic effects of software code, and indirectly, the failure of those responsible in the public sector for employing software code to make decisions to fully understand what they are buying and implementing.

One example is the case of Helen Stokes, who found that a company of data brokers by the name of RealPage Inc, had provided inaccurate and out-of-date information about her (pp 151 – 152). She had to take legal action to have her record amended, highlighting the point that it ought to be a legal requirement that such companies ought to have the burden of proof to demonstrate that their databases are accurate and truthful. In this case, RealPage argued that their violations were only technical in nature and devoid of any concrete harm that failed to establish that there were any injuries-in-fact because there was no real effect on the plaintiff and the other class members. This was rejected, for which see *Stokes v RealPage, Inc.*, 2016 WL 4681283 (E.D.Pa.) (Trial Motion, Memorandum and Affidavit); *Stokes v RealPage, Inc.*, 2016 WL 6095810; *Stokes v RealPage, Inc.*, 2016 WL 6093685 (Order on motion to dismiss denied).

Another example is the State of Michigan, which, like many other States in the United States of America, used an automated system to determine whether people claiming unemployment benefits were doing so fraudulently (pp 226 – 227). It appeared that some 20,000 people were affected. Eventually, the problems with the system were admitted (see *Michigan Integrated Data Automated System (MiDAS) unemployment Insurance Agency, Department of Talent and Economic Development and Department of Technology, Management, and Budget* (Office of the Auditor General Performance Audit Report, February 2016, Report number 614-0593-15)). Two cases illustrate the problems faced by innocent victims.

In *Bauserman v Unemployment Insurance Agency*, 2017 WL 3044120, the Unemployment Insurance Agency did not dispute that its initial determinations that Mr Bauserman was not eligible for unemployment benefits and had engaged in fraud was wrong, after it received notice from Mr Bauserman that he received a payment from his former employer that was a bonus he was entitled to while still employed by his former employer. The monies seized from Mr Bauserman were returned by the Unemployment Insurance Agency. The legal action initiated by Mr Bauserman alleged that the Michigan Integrated Data Automated System deprived him and other claimants of due process and fair and just treatment because it determined guilt without providing notice, without proving guilt and without affording claimants an opportunity to be heard before penalties are imposed. In this instance, the court reversed a previous decision refusing summary disposition and remanded for entry of an order granting summary disposition in favour of the Unemployment Insurance Agency.

The same issues arose in *Zynda v Arwood*, 175 F.Supp.3d 791 (E.D.Mich. 2016) (dated 29 March 2016), followed by *Zynda v Arwood*, 2016 WL 4593828, Unempl.Ins.Rep. (CCH) P 22,437 (dated 2 September 2016). The defendants wanted to have the action dismissed, but this was refused. Of interest are the comments by Cleland J at the September 2016 hearing (at 3, italics in the judgment):

> 'Defendants do not explain in detail how fraud determinations are currently made, nor do they explain how any improvements will affect Plaintiffs' due process concerns going forward. It strains credulity to assert that Defendants will *never again* use computer systems similar to MiDAS to make fraud determinations, even if use of the specific MiDAS system has been discontinued and staff determinations have been implemented as Defendants suggest. The implementation of staff determinations is evidently no great deviation from the earlier procedure, as Defendants admit that "[p]reviously, the Agency used MiDAS, *in addition to staff*, to issue Agency determinations and redeterminations involving fraud." (Dkt. #33-1 (emphasis added).) Defendants have given the court no basis to conclude that their current or future methods for determining fraud are any more likely to comport with due process than the procedures that the Defendants have discontinued. For example, Defendants do not indicate whether they are using some system similar to MiDAS to assist in the staff determinations, whether staff are actively involved in assessing the facts suggesting the presence of fraud, or if the staff are simply responsible for the "issuance" of the determinations in a way such that a person may rubber-stamp the findings of a computer system substantially similar to MiDAS. (*See generally* Dkt. #33-1.) Therefore, the court cannot conclude on this basis that "subsequent events make it absolutely clear that the allegedly wrongful behavior cannot reasonably be expected to recur." *See Cleveland Branch* NAACP, 263 F.3d at 531. However, even if the court were armed with these facts, it could not rule out the possibility that Defendants might resume the allegedly unconstitutional conduct. Thus, Defendants' voluntary cessation, even if entirely correct and fully disclosed herein, does not render Plaintiffs' claims moot.'

This is a refreshing comment by Cleland J about the reality of the problem, and reinforces the points made by Cathy O'Neil in this excellent book that judges and lawyers ought to consider as essential reading for the world in which we live now.

Contents

Title: **A Gift of Fire Social, Legal, and Ethical Issues for Computing Technology**

Authors: **Sara Baase and Timothy M. Henry**

Edition: **Fifth**

Date and place of publication: **2017** [the book gives a date of **2018**], **United States of America**

Publisher: **Pearson**

ISBN: **978 0 134 61527 1**

Sara Baase is Emeritus Professor of Computer Science at San Diego State University, and wrote the first four editions of this excellent text, and Timothy M. Henry, who is an Associate Professor at the New England Institute of Technology, has joined Professor Baase for the fifth edition.

This is not a book for law students, although law students would benefit from being made aware of it. Society generally would benefit if law students (and by implication law lecturers) began to join technology students in joint sessions, where technology and the law are discussed and analyzed. At present, with rare exceptions, the law does not interact with technology, and technology does not interact with the law.

The authors point out that the book is aimed at two audiences: students preparing for careers in computer science and related fields, and students in other fields who want to learn about issues that arise from the digital world.

The approach is different to many books on law – the authors adopt a problem-solving approach, by providing a description of the issues in each area, including some history. This is followed by a discussion of the concerns and problems – and this aspect is refreshing and stimulating. The authors also offer a commentary or perspective, and set out what might be the latest solutions that have been suggested or adopted. There follows a series of exercises that students might be asked to consider, followed by suggested assignments, and a further section on exercises for discussion in class. Endnotes provide yet more selected further information.

The authors comment in the preface (xvi – xvii) that students quickly find the text to be far from boring, and in fact interesting and important. Looking at the thought that has gone into this text over the years, it is not surprising that students react in such a positive way. Teaching students that have the benefit of this book must be a delight.

The constructive nature of this text more than makes up for a number of minor issues that arise from a reading by somebody from a different background. The authors are careful to point out in the preface (xvi) that the laws and cases are summarized, and no legal analysis is offered, directing the reader to the law reports and lawyers for more information. This is natural, and notwithstanding this warning, it is good that the authors introduce decisions by judges and laws into the text – doing so enriches the text. I would suggest, though, that the authors might ask a legal academic or lawyer to look over the case reports, etc for future editions. For instance, many of the cases cited do not include the full citation, only the name of the parties. This is not helpful in finding the actual judgment.

It is strongly suggested that care is taken to cite comments from judgments. For instance, the comments of Zlaket J (at 872) are quoted on page 420, the endnote merely giving the name of the case: *Arizona v Evans*. In fact, this was a judgment that was overturned by an appellate court. The citation of the case is *Arizona v Evans*, 177 Ariz. 201, 866 P.2d 869 (Ariz. 1994), which is a decision of the Supreme Court of Arizona. This was a case where Evans was stopped by police officer Bryan Sargent for driving a motor vehicle the wrong way along a one-way street in front of the police station on 6 January 1991. The police officer stopped Evans and asked to see his driver's license. Evans told the police officer that his license had been suspended. The police officer then entered Evans' name into a computer data terminal located in his patrol car. The inquiry confirmed that his driving license had been suspended, and also indicated that there was an outstanding misdemeanor warrant for his arrest. He was arrested, based on the outstanding warrant. A subsequent search of Evans' car revealed a bag of marijuana, and he was charged with possession. However, the record on the computer regarding the outstanding warrant was incorrect. The arrest warrant had been quashed by an issuing court several weeks earlier. Nobody had removed this information from the computer database. The evidence as to this failure was unsatisfactory. It was not clear whether the staff at the court had informed the police that the warrant had been quashed, and even if they had informed the police, why the police did not alter the database on the computer. Evans applied to have the charge suppressed on the basis that the police officer became aware that he had the marijuana because of an unlawful arrest. This was because the misdemeanor warrant had been quashed before his arrest. The trial judge, Brown J, granted the motion and dismissed the case.

The prosecution appealed against this decision to the Court of Appeal. The citation of this judgment is *State of Arizona v Evans*, 172 Ariz. 314, 836 P.2d 1024 (Ariz.App. Div. 1 1992). Eubank J gave the judgment and Voss PJ concurred, with Claborne J dissenting. The court reversed the decision by Brown J on the basis that the mistake was, more probably than not, made by a justice court employee and not a police officer. The rule to exclude evidence was intended to deter police misconduct, not to punish errors made by judges and magistrates. This meant the evidence should not have been suppressed.

Evans then appealed to the Supreme Court of Arizona against the decision of the Court of Appeal. The authors cite from the reported decision of the Supreme Court of Arizona. Zlaket J, with Feldman, CJ, Moeller VCJ and Corcoran J concurring, gave the judgment. Martone J dissented, emphasising that the exclusionary rule applied to police misconduct, not judicial departmental errors. The majority members of the Supreme Court of Arizona held that the trial court properly supressed the evidence found by the police officer. They said it was not relevant that the police officer acted in good faith. Emphasis was placed on the fact that the arrest was made because of negligent record keeping. The police officer arrested Evans on the basis of an arrest warrant that did not exist. The majority members of the Supreme Court of Arizona did not agree with the Court of Appeals that there was a distinction between clerical errors committed by the police and similar mistakes by court employees. They emphasised the performance of ministerial functions, not the exercise of judicial discretion.

The prosecution appealed to the Supreme Court. The citation is *Arizona v Evans*, 115 S.Ct. 1185 (1995). Rehnquist CJ delivered the opinion of the court. The Supreme Court 'granted certiorari to determine whether the exclusionary rule requires suppression of evidence seized incident to an arrest resulting from an inaccurate computer record, regardless of whether police personnel or court personnel were responsible for the record's continued presence in the police computer.' (115 S.Ct. 1185, 1189). The Supreme Court reversed the decision of the Supreme Court of Arizona. Souter and Breyer JJ concurred with the Chief Justice, and Stevens and Ginsberg JJ dissented. The majority decision reversed the decision on the ground that the purpose of the exclusionary rules is not served by excluding evidence obtained because of an error by employees not directly associated with the arresting officers or their police department. The Arizona Supreme Court was wrong to predicate the application of the exclusionary rule as a basis to improve the efficiency of the record keeping of the criminal justice system. In dissenting, Stevens and Ginsberg JJ wrote judgments that are worthy of careful reading. For instance, Ginsberg J said, at 1200:

> 'In this electronic age, particularly with respect to recordkeeping, court personnel and police officers are not neatly compartmentalized actors. Instead, they serve together to carry out the State's information gathering objectives. Whether particular records are maintained by the police or the courts should not be dispositive where a single computer data base can answer all calls. Not only is it artificial to distinguish between court clerk and police clerk slips; in practice, it may be difficult to pinpoint whether one official, *e.g.*, a court employee, or another, *e.g.*, a police officer, caused the error to exist or to persist. Applying an exclusionary rule as the Arizona court did may well supply a powerful incentive to the State to promote the prompt updating of computer records. That was the Arizona Supreme Court's hardly unreasonable expectation. The incentive to update promptly would be diminished if court-initiated records were exempt from the rule's sway.'

At the end of her dissenting judgment, Ginsberg J commented on the comments cited by the authors on page 420, at 1203:

> 'The Arizona Supreme Court found it "repugnant to the principles of a free society," 177 Ariz., at 204, 866 P.2d, at 872, to take a person "into police custody because of a computer error precipitated by government carelessness." *Ibid*. Few, I believe, would disagree. Whether, in order to guard against such errors, "the exclusionary rule is a 'cost' we cannot afford to be without," *ibid.*, seems to me a question this Court should not rush to decide. The Court errs, as I see it, in presuming that Arizona rested its decision on federal grounds. I would abandon the *Long* presumption and dismiss the writ because the generally applicable obligation affirmatively to establish the Court's jurisdiction has not been satisfied.'

That this case relates to the issues that arose in the 1990s and remains of interest, although it will be useful to refer the reader to more up-to-date judgments on the same topic. However, it is to be noted that this case was about negligent record keeping, not about the errors of software code.

The authors also consider the knock-on effects that software errors can have on others, and cite the CTB McGraw Hill software for standardized tests in schools by way of example (p 419). This is a very interesting and highly pertinent discussion, for which also see Kathleen Rhoades and George Madus, *Errors in*

Standardized Tests: A Systemic Problem (National Board on Educational Testing and Public Policy, May 2003) http://www.bc.edu/research/nbetpp/statements/M1N4.pdf. On the topic of citations of relevant further information, the discussion on privacy in chapter 2 was most interesting. The authors rightly consider the background to privacy in the United States of America at 2.3.2, but miss referencing a seminal work, that of Professor Westin: Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967). It was Professor Westin's work on this topic that caused a change in the law: surely a work that is worthy of being remembered and read today.

Chapter 5 considers crime and security, exceedingly important topics that exercise police forces and national spy agencies across the globe. At 5.7.1 a sub heading is 'French censorship'. In chapter 3, the authors consider the limitations on freedom of speech in the United States of America, yet the discussion of the French position in the context of Nazi memorabilia is slightly taken out of context, even though it is discussed in the setting of the application of the laws of one country against citizens of another country. The French law that applies to Nazi memorabilia is La loi no 90-615 du 13 juillet 1990 tendant à réprimer tout acte raciste, antisémite ou xénophobe, dite loi Gayssot (Act No. 90-615 of 13 July 1990 to repress any racist, anti semitic or xenophobic act, known as the Gayssot law). The reader really ought to be made aware of the reason for the passing of this law – based, as it is, on the suppression of the existence of crimes against humanity, which were defined at the International Military Tribunal at Nuremberg. It is strongly suggested that the authors consider amending the sub-title and put the French law into context.

A final observation relates to a topic that is now constantly at the forefront of the media: that of what are described as autonomous motor vehicles (the authors call them 'self-driving', but they mean vehicles that are driven by software code written by human beings). Discussing the topic is highly relevant, but the mix of dubious facts and opinions (pp 5 – 7) do not sit well. It is asserted that autonomous motor vehicles will save lives. There is no evidence to sustain this assertion. In fact, software code in motor vehicles has been the cause of deaths and injuries of people.

Professor Martyn Thomas indicated in a letter published in the *Financial Times*, 1 October/2 October 2017 that human drivers are, actually, 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. Professor Martyn went on to indicate that '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?'. He concluded by stating that '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.' It should also be noted that most software in 'smart' vehicles cannot detect humans reliably, either as pedestrians or cyclists.

This leads on to the most important issue regarding the use of software code in motor vehicles and how it causes death and injury of people when the software code takes a vehicle over (and continues to do so across the globe). The most important case to date is the *Bookout* case in the United States of America, in which the members of the jury decided that it was the software code in the vehicle that was responsible for taking over the motor car, taking it to top speed and killing and injuring a number of people. This case is discussed in depth in the open source practitioner textbook Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th end, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London), 6.84; 6.138; 6.155.

Exercise 8.38 is interesting. The NASA report was flawed, as demonstrated in the article written by Michael Barr, one of the experts in the case. The article was written before he was appointed an expert, and is highly relevant: Michael Barr, 'Firmware forensics: best practices in embedded software source code discovery' 8 *Digital Evidence and Electronic Law Review* (2011) 148 – 151. If motor vehicles are to be wholly controlled by software code, and the driver has no control over the vehicle at all, it will be useful for the authors to raise this issue in future editions of their text.

What is interesting about the motor vehicle industry is how reluctant manufacturers were to introduce safety features in dangerous vehicles. It took the energy of Ralph Nader in the United States of America to galvanize changes using public shame and encouragement to change attitudes – and drunk driving, which is appalling, could be avoided by including suitable safety measures in a vehicle to prevent a driver from starting the car, but manufacturers choose not to introduce such safety features.

The authors correctly discuss the trolley problem (p 7), but without citing Philippa Foot, 'The Problem of Abortion and the Doctrine of the Double Effect' in *Oxford Review*, Number 5, 1967, 5 – 15. It would be good if the pioneering work of this woman were to noted.

These minor considerations apart, this is an excellent text that ought to be in the hands of law students as well as technology students. May of those that teach courses that utilize this text and those attending such courses have much enjoyment and pleasure in learning from it – the pleasure must be to take part in such an exercise and responding to the numerous well-thought out questions and exercises at the end of each chapter.

Contents

Title: **Electronic Disclosure Law and Practice**

Authors: **Michael Wheater and Charles Raffin**

Contributors: **Jack Dillon, Barrister, Hardwicke; Emma Hynes, Barrister, Hardwicke; Charles Thompson, Barrister, Hardwicke**

Researcher: **Keifer Conroy, BA (Oxon)**

Edition: **First**

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

Publisher: **Oxford University Press**

ISBN: **978 0 19 877892 9**

As the first decade of the twenty-first century unfolded, it rapidly became apparent that the digital world was becoming part of every day life. We now live in a physical world and a digital world, and it is incumbent on legal academics, lawyers and judges to understand the world in which we live, and to deal with it competently. That this has not been the case and remains of significant concern in 2017 should raise questions of proficiency to practice. Until such time as the legal profession begins to take these two topics seriously – *Electronic Disclosure* and *Electronic Evidence* – we at least have some textbooks to provide guidance to those that know they need to know.

As the authors point out in their Preface, the book has been a long time in the writing. Deciding on a date for publication is all very well with this topic, but no sooner do you reach the hallowed date, when another change of such significance pops up, that it is necessary to ask the important question about whether to defer publication. However, there comes a time when the pressing need to inform and educate the profession overrides the desire to be comprehensive. The authors have grappled with this conundrum to a point, as they explain (no doubt the discussion in chapter 7 on Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88 and the British leaving the EU caused adjustments – the additional text is just about right, given the uncertainty at the time of writing), and the publishers have finally presented the profession with a thoroughly useful text.

The authors and contributors are to be congratulated on a text that a seasoned e-disclosure lawyer will appreciate, but also acts to provide a primer to the novice – if there any novices in 2017 – there should not be any, but the comments by Gloster LJ in the Foreword make it clear that judges continue to face incompetence on this topic.

The text includes all that one would expect from a book on this topic for lawyers, and the authors wisely exclude explanations of the various types of software used in the e-disclosure process. Given the technology changes so frequently, such a discussion would quickly date. The coverage, in chapter 2, of the nature and types of electronic data are sufficient for the practitioner in need of entering the world in which the client lives and which lawyers use, but fail to understand.

As to be expected, the principles of e-disclosure set the scene, in which the concept of 'reasonable search' is highly significant and not always well understood. Many, when initiating legal action, fail to understand the vast amount of electronic data that will need to be searched for relevant materials, and many clients also fail to understand their duties to prevent the destruction of data once litigation is contemplated or initiated, for which see 3.79 fn 113. 4.60 – 4.62.

Practical issues such as privilege are given detailed consideration (chapter 5), as well as the disclosure application (chapter 6). Cross-border issues (chapter 7) are highly significant – almost every-day issues – that the lawyer needs to consider, including blocking statues, and the French position is noted (for future editions, the authors might like to note that the case of *In re Advocate Christopher X*, Cour de cassation chambre criminelle du 12 décembre 2007 n°07-83228 was translated into English and published in volume 7 (2010) of the journal, pp 130 – 133). Regarding the discussion on banking secrecy, data privacy and data protection, it will be of interest to know if the proposed *Convention on Electronic Evidence*, published in volume 13 of the journal (2016) at S1 – S11 will be of any help in the future.

Part III covers the practical considerations that lawyers need to be aware of regarding e-disclosure in detail. Any lawyer new to this topic will benefit from the care put into these eight chapters, which include the presentation of evidence in legal proceedings as touched upon by Gloser LJ in her Foreword. Presentation in legal proceedings (chapter 15) is an interesting topic in itself, given the prejudice that can occur in absence of range of issues that apply, comprehensively covered by Dr Damian Schofield in his article 'The use of computer generated imagery in legal proceedings', 13 *Digital Evidence and Electronic Signature Law Review* (2016), 3 – 25.

An interesting aspect of the entire process of e-disclosure, from the moment the client steps into the office and agrees to initiate legal action, until the fist day of day of the trial (if matters are not resolve informally first), it is clear that the litigator has had to extend their role to include project management. This is a clear lesson from this text, and lawyers need to be aware of this significant change in their practice, if they have not already done so.

One minor comment on the Foreword by Lady Justice Gloster. Dame Elizabeth Gloster correctly identifies the need for lawyers to be familiar with electronic disclosure. The topic was covered in the first three editions of *Electronic Evidence* (2007, 2010 and 2012), although only in terms of relevant case law, and therefore nowhere near as comprehensively as in this first-rate text. As the fourth edition of *Electronic Evidence* was also published this year [see earlier book report], it is to be sincerely hoped that lawyers and judges will also take cognizance of this topic for the good of their clients and justice.

This is an important book by practicing barristers that all practitioners ought to have on their book-shelves, including arbitrators, for all forms of legal action invariably include evidence in electronic form.

Contents