Title: **Click Here To Kill Everybody Security and Survival in a Hyper-connected World**

Author: **Bruce Schneier**

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

Publisher: **W. W. Norton & Company, Inc.**

ISBN: **978 0 393 60888 5**

This book by Bruce Schneier acts on two levels for lawyers and judges. First, it alerts those in the legal profession that do not know about the world in which we now live (comprising the vast majority), about the lack of substantive law to protect citizens and the failure of procedural law to require owners of software code to reveal the causes of injury and death. On another level, it informs lawyers of the precarious nature of the duties they owe to their clients regarding the confidentiality of their client files.

Every lawyer should read with Schneier's monthly *Cryptogram* and keep a close watch on the web site run by Brian Krebs. When a problem occurs, Schneier and Krebs invariably pursue the facts until they understand them fully, and then report on the issue in detail – the sort of detail one would expect a court to establish in the absence of lightweight media reports.

For the reader that is not aware of Bruce Schneier and his work, this book is a must-read, as always. In the context of this journal, the text, centred on the United States of America, considers the failure to respond politically to surveillance capitalism that is now pervasive; considers the position of the security services in relation to the proper security of software code and the digital infrastructure, and alerts the reader to the ravages of relying on software code and the development of the Internet of Things, by which every aspect of our lives are recorded by people we do not know, exposing everybody to being disrupted at a time decided by the attacker. When a software failure disrupts daily life, most people quickly forget about the experience, and probably could not mention the last software problem that interrupted everyday life, yet such attacks occur frequently – and few people understand how necessary it is to resolve this issue. Reading this text will enable the uninformed reader to understand the world in which we live now.

It is not proposed to consider the practical and political issues properly raised by Schneier in this book. What is considered is why the legal profession ought to be aware of it.

To begin with, Schneier sets out an important aspect about software code that few lawyers and judges understand (p 25): that computers are extensible with three ramifications:

> (1) Extensible systems are difficult to secure.
>
> (2) They cannot be externally limited – which is why Digital Rights Management is poor at protecting copyright – in other words, software code cannot be constrained because it can be repurposed, rewritten or revised.
>
> (3) Every device can be upgraded with additional software features, which add insecurities.

In setting out these three issues, Schneier seals the fate of wanting to achieve a more secure digital world (as much as the reviewer agrees with the author). The scale of the problem is sufficiently illustrated with two examples: (i) (p 29), where hackers penetrated the network of a casino by getting in through a fish tank connected to the internet, and (ii) (p 116) where the oil pressure in the Baku-Tbilsi-Ceyhan oil pipeline was increased by gaining access to the control system to cause an explosion, then the hackers hacked into the sensors and video feeds that monitored the pipeline. The purpose of this action was to prevent operators from realising the explosion had occurred. There was a time lapse of 40 minutes before people in the control centre were aware of what had happened.

The ramifications for establishing causation in civil litigation and guilt or innocence in criminal proceedings are obvious.

In seeking a more secure digital world, it is possible to point to the failure of the law to provide for adequate remedies when software code is at issue: such as medical devices, motor vehicles, aircraft, computers and so on. Litigation is one of the remedies suggested (p 121), but unfortunately there are problems: judges rarely agree for software code to be disclosed to the other party – many judges accept the argument that the code is secret and proprietary and should not be reviewed; well-financed companies will prevaricate and use every means possible to delay the litigation, thus causing the other party (if poorly funded) to give up or accept an out-of-court remedy that includes a confidentiality clause; the substantive law relating to liability is woefully inadequate, and given the problems with politics and the substantial lobbying undertaken by the software behemoths of the twenty-first century, it is doubtful that this will change in the short term.

The author refers to the possibility that software (p 132) and the internet (p 182) might kill people, and suggests the situation will change once this occurs. In this respect, as much as it would be nice that Mr Schneier was correct in this assumption, the position is less than satisfactory. People have already been killed and injured by software, and nothing has been done about it (see chapter 6 of *Electronic Evidence* for a discussion of examples).[1] Nothing has changed. Indeed, the two Boeing 737-8 MAX flights that have crashed killing 157 (Ethiopian airlines, 29 October 2018) and 189 (Lion Air, 10 March 2019) illustrates and emphasises our reliance on software code. Both are attributed to problems relating to the new software called Maneuvering Characteristics Augmentation System and how it interacts with a physical device, although we await the final reports to understand the correct position. This is why this book is important, and why the legal profession ought to be aware of the world in which we now live, and to join in with the forces for change.

This leads on to the issue of 'trust', which Schneier refers to (pp 190; 207 – 208). We trust in the absence of knowledge.[2] In relation to the law and how judges and lawyers respond to the world of software code, not only do they need to understand that software code is ubiquitous, but it is essential to have a better grasp of the wider issues that we face, as illustrated in this book. The concluding comment, that policy makers should understand technology (p 221), is obvious, but sadly lacking – and the legal profession needs to understand the issues in the same way, but do not.[3] Arguably technologists already are involved with making policy (p 222) – it is just that the right technologists are not well represented, as illustrated during the Morecombe and Wise Christmas Show in 1972:

> André Previn (called Andrew Preview in the sketch) asks, when listening to Eric Morecombe play, 'What, what were you playing?'
>
> 'The Grieg piano concerto,' Eric replies, and continues playing.
>
> 'But you're playing all the wrong notes,' André Previn protests.
>
> At which point Eric stands up, grips the illustrious André Previn by the lapels of his dinner jacket, and says in mock menace: 'I'm

[1] 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), https://humanities-digital-library.org/index.php/hdl/catalog/book/electronicevidence.

[2] 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.

[3] It might surprise the non-legal reader to know that lawyers across the globe are certified as competent to practice, even though they have not been taught electronic evidence (which now forms part of the evidence in virtually every criminal prosecution and civil case in every jurisdiction), and calls to include the topic has been ignored: Denise H. Wong, 'Educating for the future: teaching evidence in the technological age', 10 *Digital Evidence and Electronic Signature Law Review* (2013) 16 – 24, Deveral Capps, 'Fitting a quart into a pint pot: the legal curriculum and meeting the requirements of practice', 10 *Digital Evidence and Electronic Signature Law Review* (2013) 23 – 28, both at https://journals.sas.ac.uk/deeslr/issue/view/310 .

> playing all the right notes, but not necessarily in the right order.'[4]

Many people are writing and saying the right things, but few policy makers and politicians are listening.

Finally, judges and lawyers need to read pages 20 – 22, headed 'Most software is poorly written and insecure'. With these few words, Bruce Schneier sums up the irrationality of the legal presumption prevalent in common law jurisdictions that computers are reliable (for which see chapter 6 *Electronic Evidence*).

Now it is for the judges and lawyers. The Right Honourable Lord Justice Singh is quoted in 'Viewpoints' published in *Counsel*, March 2019, pp 17 – 18 as follows:

> 'I think the important thing for a judge is to have curiosity about the world and all the different people who live in it.'

It is to be hoped that a sufficient number of judges and lawyers share this sense of exploration.

Title: **The Age of Surveillance Capitalism The Fight for a Human Future at the New Frontier of Power**

Author: **Shoshana Zuboff**

Date and place of publication: **2019, United States of America**

Publisher: **Public Affairs, Hatchette Book Group (published in Great Britain by Profile Books Limited)**

ISBN: **978 1 78125 684 8**

eISBN: **978 1 78283 274 4**

This excellent book provides an important general introduction into modern neo-feudalism (pp 43 – 44). Professor Zuboff demonstrates how people in control of legal entities (with rights but no duties, p 327), energetically pursue lawlessness to achieve their ruthless objectives of ever-greater wealth, to the detriment of the employees and contractors they employ (p 103). Security has trumped privacy (p 113), and the organs of the United States government have ensured that surveillance exceptionalism has expanded (pp 115 – 120). The software giants have understood the Dispossession Cycle, the four stages of which are incursion, habituation, adaption and redirection (pp 138 – 155). The combination of the failure of legislators to understand the world in which they live and how the software businesses have manipulated them, and weak regulators and judges failing to take robust attitudes towards the behemoths, has meant life has become a commodity for massive profit.

The range of substantive legal issues that arise from this book are extensive, including, but not limited to privacy; data protection; social exclusion (for instance, if you want to buy tickets to the tennis at Wimbledon in the future, you may only be allowed to do so through the internet, which will mean many hundreds of people without access to the internet, for whatever reason, will be excluded from attending in future[5]); unreasonableness of trading terms; monopolies and enforcement of contracts by which the provider retains extraordinary control over objects (e.g. motor vehicles that can be disabled remotely, pp 218 – 222).

For this journal, the importance of this book is in exposing the reality behind the technology of today, which should inform lawyers and judges of the importance of discovery or disclosure of software code in legal proceedings,[6] because software leviathans own the products of the surplus of our lives (in the words of the author). This now includes motor vehicle manufacturers – the vast increase in software code included in vehicles is no accident – the manufacturers have learnt from the software companies selling 'free' services such as search engines and social networking sites, which means that the motoring surplus is also to be exploited. This is where legislators should be in control – to make them

[4] https://www.bbc.co.uk/programmes/p01nmgjx .

[5] Murad Ahmed, 'Wimbledon set to abandon tradition and serve up online ballot for tickets,' *Financial Times*, Saturday 20 April/Sunday 21 April 2019, 1.

[6] As indicated in 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.

give up and control their secrets. This should be of central concern to lawyers and judges today, because the software companies now enjoy unprecedented power that has been shaped in secret. The reality is obfuscated by rhetoric camouflaged by technology (p 360), and the legal system does everyone a disservice by undervaluing the effects, or, even worse, of failing to understand the effects of such behaviour initiated behind the safety of the corporation (pp 377 – 378).

This book is essential for all lawyers. It is a realistic introduction into the world in which we have been made to live. Without such background, lawyers remain ignorant and will never be able to assert the rights of their clients – indeed, there is a significant problem with lawyers failing to understand the most basic issues relating to electronic evidence,[7] and if this continues, life will become progressively more one-sided.

One minor point of disagreement: Professor Zuboff refers to the 'real world' as if the digital world is not real. We live in the physical world and the digital world, as her text so aptly describes.

Title: **Invisible Women Exposing data bias in a world designed for men**

Author: **Caroline Criado Perez**

Date and place of publication: **2019, London**

Publisher: **Chatto & Windus**

ISBN: **978 1 78474 172 3**

This excellent book is not about the law, but about how fifty per cent of the population are largely ignored – but indirectly. Perez has written a book about how the law largely ignores causation – by ignoring women. Man is the default in life, from testing drugs and medical devices to determining the design of safety belts in motor vehicles, women and the unique physical attributes of the female body are ignored in deference to the supposedly universal male.

Mostly Americans make decisions that affect the world, and they are mostly men (p xiii). Man is the default, even though the majority of ancient hand prints in caves indicate they are of women. Additionally, we are sometimes reminded that women were important persons in the past, as with a ten-century Viking skeleton buried with a set of weapons and two horses – that men are reluctant to admit is a female (p 3) – a prevailing attitude that caused Clara Schuman to wrongly conclude that only men could be composers (p 9).

This Book Report does not need to be long, because it is an essential book for all males to read – and all lawyers. Once men realise the absurdities of how the world is arranged for men, it becomes apparent that although software code is seriously biased (and therefore should be carefully scrutinized in legal proceedings), most of the decisions made in all areas of life are similarly biased in favour of men. This should shout volumes to those involved with the law. How can it possibly be that injuries caused to a man and a woman in a collision between two vehicles are assessed equally, as if they were the same, when a woman's body is so manifestly different to that of a man?

There should be no need for this book. That there is, illustrates how much we live in a male dominated world. This book should be essential reading for all would-be lawyers and anybody that cares about fairness in legal proceedings.

Title: **Online Arbitration in Theory and in Practice A Comparative Study of Cross-Border Commercial Transactions in Common Law and Civil Law Countries**

Author: **Ihab Amro**

[7] 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)); Stephen Mason, editor, *International Electronic Evidence* (British Institute of International and Comparative Law, 2008); George L Paul, *Foundations of Digital Evidence* (American Bar Association 2008).

Date and place of publication: **2019, Newcastle Upon Tyne, United Kingdom**

Publisher: **Cambridge Scholars Publishing Limited**

ISBN: **978 1 5275 1591 8**

The title of this text implies a substantial book – at p xviii the words 'in depth' are used – but, when discounting the first 13 pages of chapter 1, it only runs to 168 pages. The book is not quite the detailed comparative study that the title suggests. The first part of chapter 1 is discounted because the author takes the reader through the developments of e-commerce and the internet generally, most of which the reader is already over-familiar. All contracts entered into other than face to face are distance contracts, regardless of the mechanism used (telegram, telex, facsimile transmission, world wide web, internet), so it is difficult to understand the claim that e-commerce differs from selling at a distance (p 12). It is to be observed that regardless of what technologists might speak about 'smart' contracts, for them to be binding, they have to have offer and acceptance, etc (p 4), which hardly makes them any different from any other form of contract.

There is a reliance on the citation of older articles and books, most of which are out-of-date; the author uses Latin tags unnecessarily and repeatedly, and occasionally the spelling of names is not correct (e.g. p 23 fn 64).

If this is an in depth comparative discussion, the list of case law is disappointing. The number of cases are in brackets: Court of Justice of the European Union (4); various states of the United States of America (7); Brazil (4); China (1); The Netherlands (1); Germany (5); Israel (1); France (4); Greece (1). This is a very small selection of case law that belies the assertion that this is a thorough discussion of relevant case law across common law and civil law countries. Notwithstanding these comments, the chapters cover relevant ground:

> Chapter 1 Cross-border electronic commerce transactions in theory and practice
>
> Chapter 2 Legal framework regulating cross-border electronic commerce and its impact on electronic contracting
>
> Chapter 3 The use of online arbitration in the resolution of international commercial disputes
>
> Chapter 4 Enforcement of cross-border online arbitral awards and online arbitration agreements in nation al courts
>
> Chapter 5 The use of online arbitration in the resolution of consumer disputes

Taking two issues by way of example, the pertinent international conventions are fully dealt with, yet the author does not consider the meaning of 'in writing' in many jurisdictions, although this journal has published a number of relevant case judgments from different jurisdictions, as a glance at the cumulative index will indicate, and three texts were available to the author to consider this topic in more detail for 46 jurisdictions:

> Stephen Mason, editor, *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012), covering: Australia, Canada, England & Wales, European Union, Hong Kong, India, Ireland, New Zealand, Scotland, Singapore, South Africa and the United States of America (although this text is now in the 4th 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))[8]
>
> Stephen Mason, editor, *International Electronic Evidence* (British Institute of International and Comparative Law, 2008), covering: Argentina, Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Egypt, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta,

[8] https://humanities-digital-library.org/index.php/hdl/catalog/book/electronicevidence.

> Mexico, Netherlands, Norway, Poland, Romania, Russia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Thailand and Turkey
>
> George L Paul, *Foundations of Digital Evidence* (American Bar Association 2008)

The other matter relates to electronic signatures. Reference to relevant case law is exceedingly rare in this text, although covered extensively, and across a significant number of jurisdictions, in 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) – which is open source,[9] and therefore a free download. Further more, from the point of view of regulations, the text by Lorna Brazell, *Electronic Signatures and Identities: Law and Regulation* (2nd edn, London: Sweet & Maxwell, 2008) – now in a third edition (too late for this book) – is very useful. It is a puzzle as to why such relevant sources were not considered.

There are problems with the layout and references in this text. It is not certain whether these are the problem of the author or the publisher. The table of cases comprises two pages; the cases are listed in no particular jurisdiction, and in block capitals; the bibliography includes a list of legislation – again, not listed in accordance with jurisdiction, and a list of web sites visited is provided at the end of the text – for what purpose, it is not clear, but this reviewer has never seen a list of URLs that appear to be meaningless, and there is no index.

The observations noted above notwithstanding, when the reader cross references the law of their own jurisdiction against the general comments in this text, they will have a more nuanced understanding of the issues for arbitrators.

Title: **Electronic Signatures and Identities: Law and Regulation**

Author: **Lorna Brazell**

Edition: **Third**

[9] https://humanities-digital-library.org/index.php/hdl/catalog/book/electronicsignatures.

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

Publisher: **Sweet & Maxwell**

ISBN: **978 0 414 06631 1**

This third edition of Lorna Brazell's work on electronic signatures and identities brings the legislation up-to-date, especially in the light of the European Union Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L257, 28.8.2014, pp. 73–114.

As the title indicates, the text concentrates on legislation and regulations, especially relating to digital signatures and other technologies that vendors attempt to sell. Signatures in general are examined in chapter 2, and then the author considers identity in chapter 3.[10] Significant discussions follow, covering technologies (chapter 4) and PKI issues (chapter 5), before dealing with the international initiatives relating to electronic signatures in chapter 6.

The shortcomings of technology and the assertions made by technologists are robustly covered. On digital signatures in particular, the author rightly points out that the certification practice statements – if people who use digital signatures are even aware of the existence of such statements – are either so short as to be meaningless, or so long as never to be read and understood (5-020). On the topic of 'non-repudiation', the author accurately observes, at 4-054:

> 'A digital signature proves only what key was used to sign, not the circumstances under which it was so used. … digital signatures have no particular advantage over other forms of electronic signature in respect of the many of the functions for which a handwritten signature is used, and in particular are significantly flawed when it comes to the

[10] Complimenting the article 'Identity and its verification', *Computer Law & Security Review*, Volume 26, Number 1, January 2010, 43 – 51 by Nicholas Bohm and Stephen Mason.

> function of identifying the signatory with confidence.'

This observation compares to the text of paragraph 7.3 bullet point three of the *Explanatory Memorandum to the Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2018*,[11] which states that a qualified signature

> 'is considered to be sufficiently secure to withstand repudiation in a court of law.'

No evidence is provided to support the assertion that it is considered to be sufficiently secure to withstand repudiation in a court of law.

Chapter 7 provides a useful resume of electronic signature law covering 67 jurisdictions. The practical problem for the lawyer arises when a client wants an analysis of electronic signature laws across a number of jurisdictions. This is a helpful analysis, but a lawyer in one jurisdiction is not able to sufficiently rely on the information in this text for the purposes of providing legal advice in respect of those jurisdictions they are not familiar with. It will be necessary to recruit a team of lawyers across jurisdictions to provide appropriate advice. Without the name of the law, it is not easy to search for and find up-to-date legislation in languages other than English – it is necessary, in many instances, to know the name of the legislation in the original language in order to identify it.

Notwithstanding the limitation noted above, the practical issues are set out in chapter 8, covering cross border transactions; jurisdiction; signature policies; choice of law; issues relating to trust providers (subscribers, relying parties); information security and record management. The technical side of regulations and standards are covered extensively in chapters 10 and 11, while the crucial consideration of evidential issues are dealt with in chapter 9. The author considers the various scenarios by which a person might raise to repudiate a signature (9-017 – 9-022), including the possibility that the certificate issued by a trust service provider is false (the VeriSign example is covered at 8-012). A number of appendices (pp 421 – 600) include model laws and other documents freely available electronically, including judgments in three cases, with the URLs usefully provided.

For anybody advising on the regulatory side of digital signatures, this book is essential, and compliments *Electronic Signatures in Law*,[12] which in turn covers the case law in depth. The two, taken together, provide an invaluable guide to the topic.

Title: **Humble Pi A Comedy of Maths Errors**

Author: **Matt Parker**

Date and place of publication: **2019, London, United Kingdom**

Publisher: **Allen Lane**

ISBN: **978 0 241 36023 1**

Software code is so closely aligned to mathematics, that lawyers need, at the haziest, an understanding of the underlying problems that can occur when dealing with evidence in digital form. This book illustrates and emphasises the problems that occur when considering electronic evidence, and what lawyers should be aware of.

The author considers a number of important examples of where software code has caused chaos: in 2004, Los Angeles Air Route Traffic Control Centre losing radio voice contact with all air traffic for 3 hours (pp 305 – 304); in 2015, it was revealed that Boeing 787 Dreamliner aircraft could potentially lose power mid-flight (pp 303 – 302); in 2017, when the F-22 Raptor fighter aircraft systems collapsed mid-flight (pp 287 – 286[13]); problems with Excel (pp 184 – 181)[14];

[11] https://www.gov.uk/eu-withdrawal-act-2018-statutory-instruments/the-electronic-identification-and-trust-services-for-electronic-transactions-amendment-etc-eu-exit-regulations-2018.

[12] (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016) by Stephen Mason, Open Access at https://ials.sas.ac.uk/digital/humanities-digital-library/observing-law-ials-open-book-service-law/electronic-signatures.

[13] For this example, see also Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edition, Institute of

missiles (pp 181 – 178); systems on US Navy warships (pp 175 – 174), and the Ariane 5 rocket (pp 30 – 25[15]).

One example was given where software code has killed and injured people: the 1987 Therac-25 medical radiation machine (pp 186 – 184[16]).

This book is a useful reminder that mathematics and software code are central to the way we live now. It is incumbent on lawyers and those responsible for setting out the qualifications necessary for lawyers to be competent to practice. This means they must understand that this topic should be a compulsory element of professional training – yet it is not.[17]

The author may be interested to know why this book has been considered for inclusion a journal relating to law – chapter 6 of *Electronic Evidence* explains all: in common law countries, there is a presumption that software code is reliable. Just imagine how dangerous such a presumption is, and has been. It is assumed that courts are the place to establish the facts, insofar as they can be ascertained. In a court of law, it is necessary for a party, when asserting a fact, to provide evidence of the fact. Yet in 1997 the Law Commission asserted that computers were presumed to be reliable without any evidence of any description. The complacency of the legal profession is astonishing.

Statistics are also covered in chapter 11. This is a timely reminder that lawyers need to appreciate the damage they can cause by not understanding them correctly, as in the notorious case of Sally Clark: *Clark, R v* [2003] EWCA Crim 1020 (http://www.bailii.org/ew/cases/EWCA/Crim/2003/1020.html). In this case, the lawyers failed to grasp the importance of the mis-use of statistics, and an innocent woman was wrongly convicted. More recently, Anthony de Garr Robinson QC, quoted statistics in his opening speech for the Post Office in the trial of *Bates v Post Office Limited* TLQ17/0455 before Mr Justice Fraser in London (a transcript of the trial will be published by this journal, and a copy is presently available at https://www.postofficetrial.com/). Mixing statistics and causation when discussing software code is dangerous, as indicated by Mr Parker. Below is what Anthony de Garr Robinson QC said in his opening speech for the Post Office:[18]

> Day 1: 11 March 2019, 98 – 101
>
> Now, in their submissions the claimants say that they will challenge Dr Worden's numerical analyses. That is to be welcomed. It will assist your Lordship to assist the soundness of his calculations. At the moment there is no engagement really by Mr Coyne with any questions of likelihood or extent, there are just some criticisms made of some of the assumptions that Dr Worden makes in his report.
>
> Now, it is worth noting that Dr Worden has a number of different calculations, some of which are more complicated and some of which involve more assumptions than others. Let me just deal with one very simple calculation. This requires no understanding of statistics or mathematics. It is set out in section 8.5 of Dr Worden's first report which starts at {D3/1/148} and it has changed a little bit in Dr Worden's second report but we don't need to address that in any detail at this stage.
>
> MR JUSTICE FRASER: I should just tell you for interest I do understand mathematics and statistics. I'm not being funny, but I do.

Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017), 6.127, https://humanities-digital-library.org/index.php/hdl/catalog/book/electronicevidence.

[14] See also *Electronic Evidence*, 'Business records', pp xii – xiii; 5.29; 7.49; 7.144.

[15] See also *Electronic Evidence*, 6.71.

[16] See also *Electronic Evidence*, 6.125.

[17] Calls to include the topic has been ignored: Denise H. Wong, 'Educating for the future: teaching evidence in the technological age', 10 *Digital Evidence and Electronic Signature Law Review* (2013) 16 – 24, Deveral Capps, 'Fitting a quart into a pint pot: the legal curriculum and meeting the requirements of practice', 10 *Digital Evidence and Electronic Signature Law Review* (2013) 23 – 28, both at https://journals.sas.ac.uk/deeslr/issue/view/310.

[18] The text that follows is taken from https://ials.blogs.sas.ac.uk/2019/06/26/the-use-of-statistics-and-software-code/.

MR DE GARR ROBINSON: No, that's very helpful, my Lord. I thought I did, my Lord, I have several maths A-levels, but I realised that my own sense of my own mathematical abilities was rather greater than it turned out to be.

MR JUSTICE FRASER: I mean this one is just a simple multiplication, isn't it?

MR DE GARR ROBINSON: Exactly.

MR JUSTICE FRASER: I think most school children would probably follow this one.

MR DE GARR ROBINSON: Exactly. It is one I understand: Over the period 2000 to 2018 the Post Office has had on average 13,650 branches. That means that over that period it has had more than 3 million sets of monthly branch accounts. It is nearly 3.1 million but let's call it 3 million and let's ignore the fact for the first few years branch accounts were weekly. That doesn't matter for the purposes of this analysis.

Against that background let's take a substantial bug like the Suspense Account bug which affected 16 branches and had a mean financial impact per branch of £1,000. The chances of that bug affecting any branch is tiny. It is 16 in 3 million, or 1 in 190,000-odd. The chances of affecting a claimant branch are even tinier because the claimant branches tended to be smaller than ordinary branches. One could engage in all sorts of calculations, but your Lordship may recall from Dr Worden's second report that he ends up with a calculation of a chance of about 1 in 427,000-odd. So for there to be a 1 in 10 chance for a bug of this scale to affect one set of monthly account for a claimant branch, one would need something like 42,000 such bugs.

Of course there's a much simpler way of doing it which really is just a straight calculation. There have been 3 million sets of monthly accounts so the chances of the Suspense Account bug affecting any given set of monthly accounts is 60 in 3 million or about 5 in a million, so to get a one in 10 chance of such a bug you would need to have 50,000 bugs like it.

But, my Lord, all the roads lead to the same basic result which is that even for a significant bug of that sort, the number of bugs that would need to exist in order to have any chance of generating even a portion of the losses that are claimed by the claimants would be a wild number that's beyond the dreams of avarice. It is untenable to suggest that there are 40,000 or 50,000 bugs of that scale going undetected in Horizon for 20 years.

Dr Worden explains that in paragraphs 643 and 644 of his first report and the reference to that is {D3/1/152}. And it is interesting, my Lord, that the claimants very sensibly do not suggest that there will have been bugs of that scale in that number operating -- lurking secretly in Horizon for the last 20 years and they don't suggest it because they can't. It's a matter of common sense. And in my respectful submission just that calculation demonstrates that the claim made at the end of paragraph 17.1 of the claimants' submissions is untenable. A combination of Horizon's impressions with the volume of transactions done in Horizon is not entirely consistent with the errors reflected in the claimants' case. In my respectful submission it is obviously inconsistent with that.

Just to be clear, that's not to say that a claimant could not have been hit by a bug. As I hope I have made clear to your Lordship, Horizon is not perfect. It remains a possibility, but the important point is how unlikely it is. But of course the question of whether an individual claimant has suffered an impact as a result of a bug is not a point for this trial. That is a breach issue to be dealt with in an individual case. This trial is about setting a

baseline for Horizon's reliability, not a final conclusion that will govern every single breach case that comes before your Lordship.

Roger Porkess has offered a number of comments below, which are reproduced with his agreement:[19]

Anthony de Garr Robinson QC: 'I have several maths A-levels'

This is another example of imprecise language. He means several maths A-level modules.

Anthony de Garr Robinson QC: 'nearly 3.1 million'

It is actually slightly *over* 3.1 million. It does not make any difference, but the imprecision is sloppy.

Anthony de Garr Robinson QC: 'Against that background let's take a substantial bug like the Suspense Account bug which affected 16 branches and had a mean financial impact per branch of £1,000. The chances of that bug affecting any branch is tiny. It is 16 in 3 million, or 1 in 190,000-odd. The chances of affecting a claimant branch are even tinier because the claimant branches tended to be smaller than ordinary branches. One could engage in all sorts of calculations, but your Lordship may recall from Dr Worden's second report that he ends up with a calculation of a chance of about 1 in 427,000-odd. So for there to be a 1 in 10 chance for a bug of this scale to affect one set of monthly account for a claimant branch, one would need something like 42,000 such bugs.'

Anthony de Garr Robinson QC: '16 branches'

He means 16 branch accounts.

Anthony de Garr Robinson QC: 'branch is tiny'

This is not right. He means 'any particular branch account'.

Anthony de Garr Robinson QC: 'The chances of affecting a claimant branch are even tinier because the claimant branches tended to be smaller than ordinary branches.'

There is a major assumption here which may well not be justified. It is that the probability of an account being compromised by an error is proportional to the size of the account. However it could be that the circumstances which give rise to an error surfacing are more likely to occur in small accounts.

Anthony de Garr Robinson QC: '1 in 427,000-odd'

A consequence of the previous point is that changing 1 in 190,000 to 1 in 427,000 cannot be justified. It does not actually make much difference, but should not have been included in the case.

Anthony de Garr Robinson QC: '1 in 10'

Now we come to the serious point. He produces the figure '1 in 10' out of a hat with no justification. Nothing that has been said so far leads to a figure anything like this.

Anthony de Garr Robinson QC: '42,000 such bugs'

This figure too is based on the invalid 1 in 10 probability.

This is then compounded by an assumption that each observed malfunction is caused by a different error in the code. This may well not be the case, particularly if the errors in the code are not fully understood and corrected following their manifestation through malfunctions.

[19] Roger Porkess is a past Chief Executive of Mathematics, Education, Innovation (MEI) for 20 years, and author or co-author of national reports on mathematics and statistics, including 'A world full of data' (Royal Statistical Society), as well as a very large number of mathematics and statistics textbooks.

> So the figure of 42,000 is completely spurious. The subsequent argument based on it is consequently less than worthless.

Anthony de Garr Robinson QC: 'Of course there's a much simpler way of doing it which really is just a straight calculation. There have been 3 million sets of monthly accounts so the chances of the Suspense Account bug affecting any given set of monthly accounts is 60 in 3 million or about 5 in a million, so to get a one in 10 chance of such a bug you would need to have 50,000 bugs like it.'

> 5 in a million is wrong. 60 in 3 million is 20 in a million or 1 in 50,000. However, it is not clear where the number 60 has come from; if Mr de Garr Robinson actually meant 16, that would give a ratio of about 1 in 190,000.
>
> However since the purpose of this calculation is then to use the fictitious 1 in 10 figure, the calculations are of no value anyway. The whole paragraph is invalid.

Anthony de Garr Robinson QC: 'But, my Lord, all the roads lead to the same basic result which is that even for a significant bug of that sort, the number of bugs that would need to exist in order to have any chance of generating even a portion of the losses that are claimed by the claimants would be a wild number that's beyond the dreams of avarice. It is untenable to suggest that there are 40,000 or 50,000 bugs of that scale going undetected in Horizon for 20 years.'

> This complete argument can and should be discounted.

Professor Peter Bishop also offered comments, which are set out below with his agreement:[20]

> Dr Worden's report cites the Suspense Account bug which had 16 failures in 3.1 million submissions. This information was used calculate the submission failure probability for the bug (around 5 10^{-6}). It was then stated that:
>
> *… for there to be a 1 in 10 chance for a bug of this scale to affect one set of monthly account for a claimant branch, one would need something like 42,000 such bugs.*
>
> The claim here is badly phrased, I think the intended phrase was:
>
> *… for there to be a 1 in 10 chance for **bugs** of this scale to affect one set of monthly account for a claimant branch, one would need something like 42,000 such bugs.*
>
> This is a complete red herring. What is actually being calculated is the number of bugs needed for a 1 in 10 chance that one set of monthly accounts is affected for any branch.
>
> The 1 in 10 criterion is a completely arbitrary figure and implies that 1 in every 10 submissions will fail (i.e. a 10^{-1} failure rate of Horizon submissions *for all branches*). This is equivalent to expecting 310,000 submissions will fail out of the total set of 3.1 million submissions. If this were the case, it would imply an average of 23 submission failures *for every Post Office branch in the UK*.
>
> Counsel later states that:
>
> *… in order to have any chance of generating even a portion of the losses that are claimed by the claimants would be a wild number that's beyond the dreams of avarice. It is untenable to suggest that there are 40,000 or*

[20] School of Mathematics, Computer Science and Engineering, Department of Computer Science, City University of London.

50,000 bugs of that scale going undetected in Horizon for 20 years.

But as we can see, this calculation does not correspond to reality, as nobody is claiming the Horizon reliability would be so poor. This is a strawman argument where an infeasible scenario is posited then demolished.

There is no rationale that relates a scenario where every one of the 31,000 branches has to experience 23 submission errors, to a situation where around 500 branch postmasters are falsely accused of fraud.

Alternative analysis

The approach used in the Worden report is completely irrelevant. The relevant statistical measure is the chance that a branch will be wrongly accused of fraud – not how likely it is that an individual submission will go wrong.

For a branch to become a suspect, it needs only one out of possibly a hundred account submissions to be incorrectly processed.

Form the Worden analysis, the Suspense Account bug caused 16 branch submission errors, so the number of similar bugs needed to get 500 branch submission error is:

= 500/16

= 31 bugs

This is three orders of magnitude less than the 40,000 to 50,000 bugs claimed to be needed by Dr Worden using the flawed criterion for the probability of failure per submission.

Are 31 residual bugs credible after 20 years? – sadly yes.

With a million lines of code and typical coding best practice we might start with 1,000 to 3,000 bugs (though concurrent transaction processing software is particularly difficult to get right as it prone to transient non-reproducible failures). So, there could easily be 31 bugs remaining undetected after 20 years

Discussion and conclusions

I find it amazing that Dr Worden's seriously flawed analysis could be viewed as credible evidence in a court of law.

Looking at the probability that an account submission can fail and saying it is tiny is meaningless on its own. By analogy, it is illogical to say that if there is only a 1 in a million chance of winning a lottery, ergo any person who claims to have won the lottery must be lying. This argument ignores the fact that increasing the number of people who buy tickets will increase the probability that *somebody* will win (even if your own chances remain the same). For example, if we know that 10 million people buy tickets, we would not be at all surprised to hear the 10 people won the lottery that week.

To perform a statistical analysis to determine whether the claimant's claims are credible, we should start from the hypothesis that *all branches* are potential victims of random Horizon failures, then ask what conditions are needed to produce 500 victims and then consider whether these conditions are credible.

We showed that only 31 bugs similar to the Suspense Account bug are needed to cause submission failure in 500 branches. This number of residual bugs is entirely credible for a complex real-time system, and in practice there could be many more than this (even in a mature 20-year-old system).

As a result of these analyses we consider that it is entirely credible that issues experienced by the 500 claimants could have been caused by flaws in the Horizon software.

These observations in relation to a few comments made by the leading lawyer for the Post Office illustrate the concerns we should have as a legal profession.

Mr Parker indicated that he has left three mistakes in the book (p 307), and also included the same competition from his previous book. Aficionados will no doubt have fun reading through such a well-written book to identify the competition. This reviewer might have noticed two errors: the claim that we have ten fingers (p 201), when most of us have eight, and the reference to two golden rules, when three were set out (p 35), although 'potato' is an interesting inclusion that probably has a meaning, and might be part of the competition. Perhaps the following are mistakes and not deliberate, or perhaps typographical errors, but included just in case they were left in deliberately:

(i) the last part of the sentence 'anti-Catholic holidays were duly anti-Gregorian calendar' (p 295) – whatever this means, and

(ii) the end of the sentence to the first paragraph on p 74 does not end on a full-stop.

This is a book that should be on the shelves of law libraries, but as with all the books included in the Book Report section of this journal relating to apparently non-legal topics, it will probably not form part of any law library.

There is only one minor observation about an otherwise excellent book that was a pleasure to read: that it refers to 'A comedy of maths errors' – yet the author refers to a total of 1,517 deaths as a result of errors, and 4 deaths relating to the results of a lottery (p 156). As fun as it might be to refer to maths and software coding as a 'comedy' of errors, perhaps more thought might have gone into the title.

Oh, and Parker is right to complain about the geometry of the football on street signs in the UK (pp 238 – 233). Apart from the fact that he is correct, it is the response by government that illustrates a disregard for truthful representations. If truthful representations are ignored, what else can be ignored?

Title: **Robot Rules Regulating Artificial Intelligence**

Author: **Jacob Turner**

Date and place of publication: **2019, Switzerland**

Publisher: **Palgrave Macmillan**

ISBN: **978 3 319 96234 4**

eISBN: **978 3 319 96235 1**

Jacob Turner has written an interesting and important book. The introductory chapter provides an outline of artificial intelligence (arguably more accurately 'algorithmic intelligence'[21]). Unfortunately, the author sadly does not cite two excellent authorities that add substance to any discussion of the topic: Joseph Weizenbaum, *Computer Power and Human Reason* (San Francisco: W. H. Freeman and Company, 1976) and Victor S. Johnston, *Why We Feel The Science of Human Emotions* (Perseus Books, 1999) – both authors have a great deal of importance to say on the topic of artificial intelligence. This omission aside, the introduction is admirably short and helpful.

The purpose of this text is to set out, in broad terms, how humanity can coexist with artificial intelligence (p 3). In discussing the response, Turner takes the reader through the features of artificial intelligence (chapter 2); discusses the legal mechanisms that might be used to address responsibility for artificial intelligence (chapter 3); sets out the arguments for rights in relation to artificial intelligence (chapter 4), concluding that society will be forced to reconsider the notion of moral rights in the light of what artificial intelligence might be capable of at some point in the future. Consideration is given to legal personality and artificial intelligence (chapter 5), taking the pragmatic view that if separate legal personality is accepted in theory for artificial intelligence (p 205), a number of unanswered questions will arise as to how such an eventually can be structured.

This leads into the last chapters, in which these matters are considered in detail. Chapter 6 discusses the possibility of creating a regulator for artificial

[21] David Harel, *Computers Ltd. What They Really Can't Do* (2000, Oxford University Press), 194.

intelligence. The author discusses whether the judges should be responsible for developing the legal response on a case buy case basis, or whether this should fall to the legislator: concluding firmly and rightly that it should be the legislator. Trends in regulations are considered by examples from a number of countries, and whether it is appropriate to regulate globally, rather than jurisdiction by jurisdiction. There is no consensus at this stage of the development of artificial intelligence: but that should not prevent nations from initiating a global talking shop to discuss the possibilities. Turner explains that the tension is whether artificial intelligence 'should be treated as an object, a subject, a thing or a person' (p 132).

The text then proceeds to controlling the creators of artificial intelligence (chapter 7), rightly pointing out that it should not be left by default to the industry – otherwise commercial corporations will ensure their interests are protected to the detriment of society generally. Regulatory codes and a licence for artificial intelligence are considered. Finally, chapter 8 identifies the need to consider controlling the creations, including identifying whether a person is interacting with artificial intelligence; whether an explanation ought to be given that artificial intelligence is involved in a process; the bias of artificial intelligence; a limitation on the use of artificial intelligence, and whether their ought, ultimately, be a mechanism by which artificial intelligence, forming part of a process, can be switched off.

This is not a premature book (p 34). As the author points out, it is important to work out how humans are going to live with artificial intelligence (p 37), especially because for the first time technology 'is interposing itself between humans and an eventual outcome' (p 64).

There is a minor point of consideration that acts in a mild way to detract from the text: Turner cites the Locomotives on Highways Act 1861 (also 1865 and 1878), at p 33 fn 125 and p 351 to argue that one has to be careful about legislation that impedes the development of technology. Arguably, the citing of this legislation is not helpful. The legislation referred to heavy steam driven agricultural vehicles of up to 14 tons in weight that caused real and practical problems on the roads at the time. The legislation dealt with these problems effectively, and was later amended to take into account the technology of the internal combustion engine – although perhaps a little less swiftly than many will have preferred.

The author does not address the practical issues of proof in legal proceedings in this text, although implies that software code can be trusted to permit the driver of a motor vehicle to switch between modes in an autonomous vehicle (p 88), when we know that software code has taken control of vehicles from the driver and taken it to top speed before crashing and killing and injuring people[22] –as it has with aircraft.[23] Introducing software code into legal proceedings is fraught with difficulties, and although the author does not discuss this topic in this book for the obvious reason that it is not part of his remit (although the 'black box' problem is rightly noted, p 325), nevertheless it is a subject that should be treated with care – indeed, consideration is given to that fact that software code is not static (p 98) – and it would be useful to touch upon the topic for a second edition, especially with the ridiculous presumption in English law that computers are reliable.[24]

Notwithstanding these minor observations, this is a text that is highly recommended and deserves a place on the bookshelf of every legislator. That Lord Neuberger has written the foreword might indicate that senior members of the judiciary will consider – and perhaps the recommendations of the Canada-United Kingdom Colloquium 2018, *Artificial Intelligence & Society, Choices, Risks & Opportunities* (Munk School of Global Affairs and Public Policy,

[22] 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), 6.84; 6.138; 6.152; 6.155; 6.226, open source at https://humanities-digital-library.org/index.php/hdl/catalog/book/electronicevidence.

[23] The Boeing 737 Max air crashes in 2018 and 2019 are probable examples.

[24] For which see chapter 6 of *Electronic Evidence*.

University of Toronto, Canada) might also be taken seriously, especially recommendation 12.[25]

Title: **Responsible AI A Global Policy Framework**

Editor: **Charles Morgan**

Date and place of publication: **2019, United States of America**

Publisher: **International Technology Law Association**

ISBN: **978 1 7339931 0 4**

The members of the International Technology Law Association that have contributed to this Framework have completed a useful exercise in considering the range of practical issues that already have arisen with artificial intelligence (AI, briefly explained at pp 19 – 24), and complements the text written by Jacob Turner also considered in this issue of the journal. Consideration is given to eight areas, each with a chapter:

Ethical purposes and Societal Benefits

Accountability

Transparency and Explainability

Fairness and Non-Discrimination

Safety and Reliability

Open Data and Fair Competition

Privacy

AI and Intellectual Property

Of interest is the reference to the book written by Thomas Friedman entitled *Thank You for Being Late: An Optimist's Guide to Thriving in the Age of Accelerations* (p 9), and the graph in this book, which is replicated on page 10, by Eric Teller, the CEO of Google's X research and development. The graph suggests that we have gone beyond the ability to understand the technologies we have invented as humans. Judging by the content of this text and the book by Jacob Turner, taken with the shocking state of education regarding practical issues such as proof of evidence in electronic form,[26] we have indeed reached beyond the ability to understand. It is now imperative that the legal profession and legislators take urgent notice of this state of affairs. Unfortunately, the response will continue to be as slow and noncommittal as the attitudes towards global warming: people have been warned for decades about this most serious of all facts that we face as a group of animals, yet continue to do little or nothing to even begin to ameliorate the position we find ourselves in.

Notwithstanding the failure to act, the discussions are of value and interest. The authors reject that AI can have legal personality (pp 74 – 76), indicating, at pages 79 – 81, that it is important to keep humans firmly in the frame when dealing with the accountability of AI systems. This discussion is taken up in more detail in the chapter on Transparency and Explainability, and is particularly important when dealing with the 'black box' phenomena that accompanies discussions of software code and AI. As nice as it is to see so many wise words written to suggest that legal entities such as corporations ought to adopt and adhere to responsibilities around accountability and governance, including guidelines, principles and codes of conduct (pp 92 – 96), the commercial sector is hardly a good example of doing anything other than only following laws – and then reluctantly.[27]

[25] https://munkschool.utoronto.ca/publicpolicy/events/the-canada-uk-colloquium/.

[26] 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), open source at https://humanities-digital-library.org/index.php/hdl/catalog/series/observinglaw.

[27] For instance, it is alleged that Uber takes a lax approach to governance, and the Arizona Self-Driving Vehicle Oversight Committee has only met twice since 2015, which tends to indicate that politicians tend not to take governance seriously either: Mark Harris, 'NTSB Investigation Into Deadly Uber Self-Driving Car Crash Reveals Lax Attitude Toward Safety', *IEEE Spectrum*, 7 November 2009 at https://spectrum.ieee.org/cars-that-think/transportation/self-driving/ntsb-investigation-into-deadly-uber-selfdriving-car-crash-reveals-lax-attitude-toward-safety. The full documents regarding this collision are available from the NTSB

Of utmost significance, it is made clear throughout the text that AI will never exist in isolation. A human being has to write the code, and this inevitably brings with it prejudices and bias (e.g pp 136; 140; 161), and it is noted that regulation of algorithms might be difficult because AI cannot be defined easily (p 181).

The topic of reliability is mentioned (p 164), and reference is made to the Independent High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy Artificial Intelligence* (European Commission, 8 April 2019). The word 'reliable' is covered twice in detail in the European Commission document:

> *Robust AI*
>
> Even if an ethical purpose is ensured, individuals and society must also be confident that AI systems will not cause any unintentional harm. Such systems should perform in a safe, secure and reliable manner, and safeguards should be foreseen to prevent any unintended adverse impacts. It is therefore important to ensure that AI systems are robust. This is needed both from a technical perspective (ensuring the system's technical robustness as appropriate in a given context, such as the application domain or life cycle phase), and from a social perspective (in due consideration of the context and environment in which the system operates). (p 7)
>
> ***Reliability and Reproducibility.*** It is critical that the results of AI systems are reproducible, as well as reliable. A reliable AI system is one that works properly with a range of inputs and in a range of situations. This is needed to scrutinise an AI system and to prevent unintended harms. Reproducibility describes whether an AI experiment exhibits the same behaviour when repeated under the same conditions. This enables scientists and policy makers to accurately describe what AI systems do. Replication files can facilitate the process of testing and reproducing behaviours. (p 17)

It is interesting that 'reliable' is not defined in *Responsible AI A Global Policy Framework*, and the word is defined in a circular fashion in the European Commission document, much as it was by Anthony de Garr Robinson QC in his opening speech in the trial of *Bates v Post Office Limited* TLQ17/0455 before Mr Justice Fraser in London (a transcript of the trial is presently available at https://www.postofficetrial.com/ and will be published in this journal), where the Post Office, through its leading counsel, claimed that the software code was 'robust'.[28]

Below is what Anthony de Garr Robinson QC said in his opening speech:

> Day 1: 11 March 2019, 87
>
> MR JUSTICE FRASER: I'm not in any way being difficult, I think we may as well just deal with it upfront at the beginning. Am I to read "robust" as meaning "extremely unlikely to be the cause", or is there more meaning to "robust" than that? Because I think whatever it is, we all have to make sure we are using the word the correct way, or the same way.
>
> MR DE GARR ROBINSON: The concept of robustness is a concept which involves reducing to an appropriate low level of risk, the risk of problems in Horizon causing shortfalls which have a more than transient effect on branches. So it involves both measures to prevent bugs arising in the first place but those measures are never going to be perfect and it includes measures which operate once a bug has actually occurred and

Document Management System at https://dms.ntsb.gov/pubdms/search/hitlist.cfm?docketID=62978&CurrentPage=1&EndRow=15&StartRow=1&order=1&sort=0&TXTSEARCHT=.

[28] Originally posted at https://ials.blogs.sas.ac.uk/2019/06/25/the-use-of-the-word-robust-to-describe-software-code/ see also the post by Peter Sommer at https://ials.blogs.sas.ac.uk/2019/06/28/robustness-and-reliability-in-computer-systems/.

triggered a result. It is both aspects of the equation. I don't say that the word "robust" necessarily means "extremely low level of risk", but what we say is that if you have a robust system it produces a result in which the system works well in the overwhelming majority of cases and when it doesn't work well there are measures and controls in place to reduce to a very small level the risk of bugs causing non-transient lasting shortfalls in any given set of branch accounts.

Day 1: 11 March 2019, 101 – 103

Now, before addressing the expert reports on robustness it is worth noting the large measure of agreement that now exists between the experts. There is no dispute about the architecture or capabilities of Horizon. There's no suggestion that Horizon lacks important capabilities or that it doesn't generally perform satisfactorily. There is no suggestion of any systemic problem lurking in Horizon.

In short, it is accepted that Horizon works well for the overwhelming majority of cases and consistently with that it is now common ground between the experts that Horizon is robust and that its robustness has improved over time and your Lordship already has the reference, it is the joint statement, the third joint statement, page 2, {D1/4/2}.

Now, what does relatively robust mean? It means robust as compared with comparable systems -- big systems, systems that keep aircraft in the air, that run power stations and that run banks.

My Lord, by the same token it is common ground that the Horizon is not infallible. It has and will continue to suffer faults every now and then. Sometimes, in a really small number of cases, those faults will have an effect on branch accounts, but it should be remembered that robustness is not just about preventing bugs from appearing in the first place, it is also about limiting the lasting detrimental effects when they do appear.

Your Lordship will hear evidence that bugs affecting branch accounts are given a high priority when they are addressed by Fujitsu. They are not ignored. And, my Lord, the evidence also shows that bugs which have an effect on branch accounts occur only very rarely indeed. There is a dispute between the experts as to precisely how rarely, but in the context of a huge system that's been in continuous operation for 20 years, that dispute in my submission does not have a material bearing on the outcome of this trial. In the overwhelming majority of cases, branch accounts will not contain a shortfall caused by a bug and the scale of bugs that would be needed to undermine that simple fact would be enormous.

Putting the point another way, the difference now being played out between the experts is at the margins. They accept that there are imperfections in the Horizon system with the result that in some rare cases bugs affecting branch accounts occur and will not be immediately fixed. The issue between them is how slight are the relevant imperfections.

A number of people have kindly responded to clarify these comments, which are set out below, with their agreement.

Professor Martyn Thomas, CBE,[29] commented:

> It seems that De Garr Robinson is using the word 'robust' tautologically, in that the software is asserted to be robust (i.e. not to have caused serious problems) and therefore it didn't cause serious problems. The excerpt at pp 101-103 is again tautological. Bugs are only 'slight imperfections' if their consequences are trivial. This is the central

[29] Fellow and former IT Livery Company Professor of Information Technology at Gresham College; Visiting Professor in Software Engineering at the Universities of Manchester, Aberystwyth and formerly Oxford and Bristol.

issue in the case, as I understand it. It is also true that bugs are only fixed when they have been detected and determined to be important. If the PO is arguing that there were no bugs or that any bugs would have been fixed, their argument is either meaningless or circular.

Mr De Garr Robinson says "Now, what does relatively robust mean? It means robust as compared with comparable systems -- big systems, systems that keep aircraft in the air, that run power stations and that run banks." But safety-critical systems that keep aircraft in the air are built to rigorous standards that far exceed the normal practices of commercial software developers and that are unlikely to have been followed for Horizon. Commercial systems, such as those used by some banks, fail uncomfortably often as the customers of TSB discovered to their cost in 2018.

Little reliance should be placed on the failure frequency in a long period of service because new defects can be introduced any time that the software is changed (whether to correct defects that have caused failures or for other reasons). A bug that caused aircraft to be grounded at Heathrow in December 2014 was in a flight data processing system that was written in the 1960s. The defect was introduced in a modification made in the 1990s that was not found in extensive testing or subsequent use but that was triggered in 2014 by particular data.

Most complex software contains many latent defects that will only cause failures under specific and rare combinations of data. It is perfectly possible that Horizon could contain defects that are not triggered by most branch transactions but that were triggered by some others.

Professor Peter Bishop[30] observed:

It could be broader and apply to the system as a whole, e.g. 'A system is robust if abnormal behaviour can be detected and rectified'. This is a personal definition, not a broadly agreed term, but I think it captures the idea that software is never going to be perfect, but we can live with it if there is some means of reducing the impact of failures.

So for Horizon we could ask:

(i) What means exist for detecting abnormal behaviour?

(ii) What processes exist to rectify to the consequences?

(iii) What means exist to identify the cause of abnormal behaviour?

(iv) What processes exist to prevent a recurrence of abnormal behaviour?

I have some experience with electronic fund transfer systems, and what I see there are separate journal logs (e.g. for individual banks and the central bank) with some form of periodic 'reconciliation', i.e. money sent from A to B should agree in both A and B journals. For Horizon, we could ask:

(i) Is there an independent (tamper-proof) journal for each sub-post office?

(ii) Can this journal be reconciled against the amount recorded within Horizon?

(iii) Is there a composite journal for the central Horizon system that can be checked for consistency against the sub-post office journals?

(iv) Is there a test environment where journals be re-run to identify the cause of a discrepancy?

[30] School of Mathematics, Computer Science & Engineering, Department of Computer Science, City, University of London.

Professor Derek Partridge[31] commented:

> I do not think that "robustness" is a particularly pertinent term. It usually refers to the ability of a software system to stand up to misuse (i.e. users entering wrong commands and/or inappropriate data) and not crash (as so many do) or deliver spurious results. A robust system should be able to take what's thrown at it, continue working smoothly and request the user (ideally with some guidance) to enter an appropriate command or valid data.
>
> This is very different from, what seems to me to be, the 'correctness' of the system, i.e., is it always functioning exactly as it should be (which, ideally, is defined in the original system specifications)?
>
> It seems to me like the very difficult issue of what appears to be a subtle error that is either activated rarely by an unknown condition, or is possibly always active but only compounds into an obvious problem on odd occasions.
>
> The Post Office Horizon system is vastly more complex than a cash machine which must broaden the scope for subtle either generally (but not always) self-correcting or very rarely occurring errors, perhaps very small errors that compound into significance.

Roger Porkess[32] noted:

> As far as I can see there are two strands to Mr de Garr Robinson's argument. Neither is valid.
>
> Strand 1
>
> > Malfunctions occur only rarely so the system is robust.
> >
> > Since the system is robust, the malfunctions cannot be the fault of the system.
>
> This is obviously a circular argument.
>
> Strand 2
>
> > If the system was to blame, the number of software errors would be so large as to be unrealistic.
>
> The figures used to support this argument are fallacious.

Specific comments:

> 'It is both aspects of the equation.'
>
> > This is the first of several places where Mr de Garr Robinson uses language imprecisely, something that I find very surprising when presenting a legal case. Something like "In both strands …" would have been better than "… both aspects of the equation …". There is no equation in sight.
>
> 'There is no suggestion of any systemic problem lurking in Horizon.'
>
> > I do not think this statement is true. Clearly some problems do remain.
>
> 'systems that keep aircraft in the air'
>
> > This is a highly inappropriate analogy. Excepting the new 737, aircraft do not fall out of the sky because their systems are 100 per cent robust. No level of failure, however rare, is acceptable. By contrast the evidence shows that the Horizon software is not completely robust, for whatever reason.
>
> 'In the overwhelming majority of cases, branch accounts will not contain a shortfall caused by a bug and the scale of bugs that would be needed to undermine that simple

[31] Professor Emeritus, past Chair of Computer Science at the University of Exeter.

[32] Past Chief Executive of Mathematics, Education, Innovation (MEI) for 20 years, and author of a number of books on maths, including (with Sophie Goldie), *Cambridge International AS and A Level Mathematics Pure Mathematics 2 and 3* (Hodder Education, 2010), and author or co-author of national reports on mathematics and statistics, including 'A world full of data' (Royal Statistical Society), as well as a very large number of mathematics and statistics textbooks.

> fact would be enormous.'
>
> Two points here.
>
> > The fact that most branch accounts are correct is completely irrelevant.
> >
> > The calculation of the number of bugs does not hold up.

The trial has now ended. The judgment is expected in the autumn of 2019.

In 1997, the Law Commission decided that writers of software code wrote perfect code, because it introduced the presumption, that included computers by implication (or more accurately, digital data), that, 'In the absence of evidence to the contrary, the courts will presume that mechanical instruments were in order at the material time'. Politicians decided to replicate the presumption for criminal proceedings by passing section 129(2) of the Criminal Justice Act 2003. No evidence was put forward by the Law Commission to substantiate the assertion that computers were 'reliable' (this is the word that is often used), and proposals for reform have not been take up.[33] This presumption illustrates the cognitive dissonance of the Law Commission and judges.[34] Judges accept computers are 'reliable', yet allow companies that write software code to include a contract term in the software licence that clearly states that writers of software code are not perfect. Here is an example:

> *The Licensee acknowledges that software in general is not error free and agrees that the existence of such errors shall not constitute a breach of this Licence*

So, who is correct? Is it the Law Commission and judges who agree that software is 'reliable' (whatever that means – no judge has ever determined what 'reliability' is, for which see chapter 6 in *Electronic Evidence*)? Or is it the people responsible for writing software code, who explicitly state that software is generally not error free? Lest the reader consider this issue is only a problem for the jurisdictions comprising the United Kingdom, consider the Canada Evidence Act (R.S.C., 1985, c. C-5). Clause 31.2(1) provides for requiring the 'proof of the integrity of the electronic documents system by or in which the electronic document was recorded or stored'. However, the difficulty lies in the provisions of 31.3(a):

> For the purposes of subsection 31.2(1), in the absence of evidence to the contrary, the integrity of an electronic documents system by or in which an electronic document is recorded or stored is proven
>
> > (a) by evidence capable of supporting a finding that at all material times the computer system or other similar device used by the electronic documents system was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic document and there are no other reasonable grounds to doubt the integrity of the electronic documents system;

The words 'operating properly' stand out. The presumption remains in Canadian legislation, yet 'operating properly' is not defined,[35] although Walsh J in *Her Majesty the Queen v. Dennis James Oland* 2015 NBQB 245 dealing with a trial within a trial regarding the admission of evidence before trial, noted, at [63]:

> 'I am satisfied on circumstantial evidence that that system was working properly - because it

[33] Stephen Mason, 'Electronic evidence: A proposal to reform the presumption of reliability and hearsay', *Computer Law and Security Review*, Volume 30 Issue 1 (February 2014), 80 – 84.

[34] 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.

[35] Judge Castor H.F. Williams refers to 'operating properly' in *R. v. Adams*, 2009 NSPC 15, but does not define what he meant by the term; *R. v. Nardi*, 2012 BCPC 0318, *R. v. Nde Soh*, 2014 NBQB 20 and *R. v. Miro*, 2016 ONSC 4982 for the same point; in a ruling on the admissibility of digital data from Blackberries, Band J found the presumption to operate without defining what it meant in *R. v. Avanes*, 2015 ONCJ 606; Baltman J referred to circumstantial evidence that a computer was operating properly in *R. v. C.L.*, 2017 ONSC 3583.

> would necessarily be designed and relied upon to accurately record that information given the nature and purposes of that information (i.e. phone usage records kept in the ordinary and usual course of business) and the nature of the business (i.e. by a major communication service provider).'

He also considered, at [72], that the 'system was operating properly given the nature of the resulting information, i.e. it did what was expected of it.' In making these comments, the judge assumed that software code was necessarily designed and relied upon to accurately record data.[36] Notwithstanding this discussion regarding 'operating properly', the 31.3(a) presumption tends to be fairly easily satisfied, and in many cases does not require expert evidence, although as more complex electronic evidence is necessarily introduced into legal proceedings, it follows that there are more digital evidence professionals involved.

All of this has an effect on the discussion of AI, but neither the European Commission High-Level Expert Group on Artificial Intelligence nor the authors that have taken part in this helpful book has addressed this issue – neither has even referred the reader to what little literature there is on the topic.

To sum up, this is a useful text that cites a good range of articles, books and special reports that help the reader begin to understand the enormity of the discussions about AI. The authors are not afraid of disagreeing about whether AI should have legal personality, and emphasise the need for suitable urgent work to be undertaken on this topic before the opportunity is missed. Notwithstanding that Elaine Herzberg was killed by motor car under the control of software code on 18 March 2018 (p 173), it is not correct that the person sitting in the drivers seat was a male: it was Ms Rafaela Vasquez.[37]

It is a must-read for all legislators and lawyers.

Title: **Human Compatible AI and the Problem of Control**

Author: **Stuart Russell**

Date and place of publication: **2019, United Kingdom**

Publisher: **Allen Lane**

ISBN: **978 0 241 33520 8**

The accolades that accompany this book by Stuart Russell are richly deserved. This useful book illustrates the problems that might occur with general purpose human level AI systems, if such systems ever come into being, and certainly if such developments occur without taking into account the powerful and lucid comments made in this excellent book:

> Chapter 1 If we succeed
>
> Chapter 2 Intelligence in humans and machines
>
> Chapter 3 How might AI progress in the future?
>
> Chapter 4 Misuses of AI
>
> Chapter 5 Overtly intelligent AI
>
> Chapter 6 The no-so-great AI debate
>
> Chapter 7 AI: Different approach
>
> Chapter 8 Provably beneficial AI
>
> Chapter 9 Complications: Us
>
> Chapter 10 Problem solved?
>
> Appendix A Searching for solutions
>
> Appendix B Knowledge and logic

[36] *Thacker v Iamaw, District Lodge 140*, 2016 CanLII 62600 (BC LA) and 2017 CanLII 79369 (CA LA) where the arbitrator made similar assumptions. Such an assumption is not necessarily warranted, for which see Luciana Duranti and Corinne Rogers, 'Trust in digital records: An increasingly cloudy legal area', *Computer Law and Security Review*, (2012) 28(5), 522 – 531.

[37] Richard Speed, 'Cops: Autonomous Uber driver may have been streaming The Voice before death crash', *The Register*, 22 June 2018, at https://www.theregister.co.uk/2018/06/22/uber_fatal_crash_driver_distracted_police_report.

Appendix C Uncertainty and probability

Appendix D Learning from experience

Professor Russell has written a text that sets out the brief history of artificial intelligence; provides an insight into the limitations of the technology; explains the current techniques in artificial intelligence, and discusses the central problem: how to control artificial intelligence.

For this discussion alone, the book is highly recommended.

The book is also relevant for the purposes of this journal because, as will be observed from reviews of other books in this year's journal and in previous volumes, the technical and the law fail to coincide. This is to be heartily regretted.

This failure is a serious problem. Of course, it is not a problem if you never face prosecution where electronic evidence is relied upon by the prosecution. However, if you are prosecuted, you will find some very unpleasant surprises that are a significant cause for concern, as many people discover.[38] Three issues arise in this context: the lack of education of investigating personnel, lawyers and judges;[39] the failure of successive governments to properly fund the police and digital forensic services, and the presumption that computers are reliable.[40]

Software code kills and injures people.[41] It is also not understood properly, as demonstrated in the case of the prosecution of nurses at the Princess of Wales hospital in Wales[42] and the present Group Litigation of *Bates v Post Office Limited*.[43] This means the discussion about the future of software programing is all the more significant.

If legal systems explicitly accept, as in England & Wales, or implicitly accept, as in many civil law systems, that computers (most significantly, software code) is reliable, then a future with general purpose human level AI systems will make lives even more miserable. An example is the case of Seema Misra.[44] Seema Misra was prosecuted by the Post Office because, it was claimed, she stole £74,609.84 belonging to Post Office Limited. Seema Misra was found guilty and sentenced to fifteen months' imprisonment. The Criminal Courts Review Commission will consider this case, among other cases relating to the Post Office and the Horizon system, after the end of the present Group Litigation.

Regardless of the nature of the other evidence in this case, what is striking are the comments made by Warwick Tatford, the barrister for the prosecution. In courts across the globe, the defence has the right to silence, yet consider the comments by Warwick Tatford on Day 1 Monday 11 October 2010, 23H-24A:[45]

> 'She does not have to give evidence of course, but the Crown has hoped that the defence might be at least guided by instructions coming from the person responsible for the computer system at this office.'

In this case, it was asserted that Seema Misra was the person responsible for the computer system at this office, yet the recent Group Litigation has established clearly that Fujitsu and the Post Office could enter the computer in a local office remotely and alter anything in the sub-postmistresses system. This was also known by the Post Office and Fujitsu at the time of this trial. The fact was, at the time of the trial, that

[38] In the context of the Post Office Horizon debacle, see the stories of lives ruined at https://www.postofficetrial.com/.
[39] For references, see the review of Bruce Schneier's book, *Click Here To Kill Everybody Security and Survival in a Hyper-connected World*, above; see also *Electronic Evidence*, 'Analysis of a failure' at 9.90-9.95.
[40] For references, see the review of Matt Parker's book, *Humble Pi A Comedy of Maths Errors* and *Responsible AI A Global Policy Framework*, edited by Charles Morgan, above.
[41] *Electronic Evidence*, chapter 6 for examples.
[42] *Electronic Evidence*, 'Analysis of a failure' at 9.90-9.95.
[43] For references, see the review of Matt Parker's book, *Humble Pi A Comedy of Maths Errors* and *Responsible AI A Global Policy Framework*, edited by Charles Morgan, above; also Tim McCormack, 'The Post Office Horizon system and Seema Misra' 13 *Digital Evidence and Electronic Signature Law Review* (2016), 133 – 138, https://journals.sas.ac.uk/deeslr/issue/view/336.
[44] *Regina v Seema Misra*, T20090070, In the Crown Court at Guilford, Trial dates: 11, 12, 13, 14, 15, 18, 19, 20, 21 October and 11 November 2010, His Honour Judge N. A. Stewart and a jury, 12 *Digital Evidence and Electronic Signature Law Review* (2015) Introduction, 44 – 55; Documents Supplement, at https://journals.sas.ac.uk/deeslr/issue/view/328.
[45] https://journals.sas.ac.uk/deeslr/article/view/2198.

Seema Misra and other post-masters and post-mistresses did not have control over the systems in their shops.

Additionally, Warwick Tatford's comments about computers in the discussion with the judge regarding disclosure (Day 1 Monday 11 October 2010, 21A-C; 23H-24A), and in his opening speech, highlight a misunderstanding about how computers and computer systems fail, and indirectly allude to the presumption. Warwick Tatford said (Day 1 Monday 11 October 2010, 49F-H):

> 'So it has got to be a pretty robust system and you will hear some evidence from an expert in the field as to the quality of the system. Nobody is saying it is perfect and you will no doubt hear about a particular problem that was found, but the Crown say it is a robust system and that if there really was a computer problem the defendant would have been aware of it. That is the whole point because when you use a computer system you realise there is something wrong if not from the screen itself but from the printouts you are getting when you are doing the stock take.'

To assert that a complex system, which the Horizon software appears to be, is 'robust', the prosecution ought to have produce evidence to establish what was meant by 'robust' and the truth of the claim. No evidence was produced to demonstrate that the system was 'robust', or to establish the 'quality' of the system – none of the tests for complex systems set out in chapter 7 of *Electronic Evidence* (as it is now – it was chapter 4 at the time of this trial) were considered. The Post Office also failed to produce any evidence regarding the operation of the operating environment and the reconciliations, error rates, controls, and relevant internal audit processes used to ensure integrity, and to provide details of the various up-dates that fixed problems with the software.

Much of the evidence in this criminal trial has now, indirectly, been challenged in the second trial of the Group Litigation – yet there is no indication from the Law Commission what, if anything, it intends to do to alter this assertion.

The lay reader might justifiably assume that courts are places for evidence to be tested; yet this is not always the case. Consider the case of *Bernt Petter Jørgensen v DnB NOR Bank ASA*, Journal number 04-016794TVI-TRON, Trondheim District Court, 24 September 2004 (a case from Norway).[46] A thief stole a number of cards, and where the customer claimed the PIN was not written down on or near the card, the trial court accepted the evidence provided by the bank, and found against the plaintiff. It does not appear that the decision in this case was appealed. Assistant Judge Leif O. Østerbø who tried the case, offered a number of comments in relation to evidence that was never submitted to the court:

> 'It is *assumed* that the standard security systems that are used are effective. However, according to Jørgensen, no cases have been documented that demonstrate the implementation of the systems are secure.
>
> The court refers in this respect to the fact that banks are subject to supervision and operate a comprehensive internal control work, and the witness Haugstad's explanation that both the standards and the practical implementation are revised thoroughly and regularly. In that regard, Haugestad explained that the systems are subject to annual audits. The Banks Control Center (BSK), in addition to the major international card companies, conducts such audits.
>
> *The court does not find that there is reason to accept that the banks' security systems are in doubt*. Although the implementation of a system necessarily involves opportunities for errors, the court cannot see that this involves

[46] For a translation into English, see *Digital Evidence and Electronic Signature Law Review* 9 (2012), 117 – 123, http://journals.sas.ac.uk/deeslr/article/view/2013; also see Maryke Silalahi Nuth, 'Unauthorized use of bank cards with or without the PIN: a lost case for the customer?', *Digital Evidence and Electronic Signature Law Review* 9 (2012), 95 – 101, https://journals.sas.ac.uk/deeslr/issue/view/309.

> significant practical risk for customers with cards.' (Italics added)

The point is, the purpose of a trial is to test the evidence. Should a judge *assume* that the standard security systems used by the bank were effective in the absence of any evidence? Should a judge accept *untested* assurances that audits actually take place, not knowing whether: (i) such audits are conducted internally or by the Banks Control Center, (ii) the audits revealed problems that might affect the systems for ATMs and PINs, and (iii) whether the audits were conducted by people with appropriate qualifications. Can a judge conclude that there was no reason to doubt the bank's security systems could be at fault without appropriate evidence as a foundation to reach such a conclusion?[47] The fact is, audits are important,[48] as is examining the software code to establish causation.[49]

This leads on to rationality and reasoning, as discussed by Professor Russell (pp 20 – 32). Consider rationality and reasoning in the context of software code and legal proceedings. The Law Commission, in their 1997 paper,[50] decided that there was a trade-off to be made when it came to proof in legal proceedings. The legal presumption reads:

> 'In the absence of evidence to the contrary, the courts will presume that mechanical instruments were in order at the material time.'

This presumption includes software code.[51] The trade-off is weighted heavily in favour of the prosecution in criminal proceedings, and can be a significant difficulty for claimants in civil proceedings, as the *Bates v Post Office Limited Group* Litigation demonstrates.

If the suggestions put forward by Professor Russell are followed up, as discussed in chapters 7 and 8, controllable general purpose human level AI systems might be possible. However, the evidence does not predict all will be well. Professor Russell mentions privacy tangentially throughout the book, more particularly at pp 70 – 71 and 127 – 129 (relating to the GDPR[52]), yet a casual search using any search engine on the internet will rapidly bring up numerous examples of how data protection legislation only deals with a minute fraction of infractions that occur after the event.[53] The legislation will have a persuasive effect on organizations to put processes and procedures in place to mitigate the possible loss of personal data, but it is not a matter of if personal data is exposed, it is a matter of when.[54] No consideration is given to the hundreds of thousands of connected private cameras and listening devices inside and outside private homes that monitor activities constantly, and are not subject to legislation. Yet it will be these devices that will also be connected to general purpose human level AI systems – to whose detriment and for the benefit of whom?

The interconnectedness of devices, including motor vehicles, will cause additional problems if general purpose human level AI systems become a reality – that is assuming the solutions presented by Professor Russell are not adopted. Already people have been killed and injured by motor vehicles being driven with degrees of autonomy – that is, motor vehicles controlled by software written by human beings that politicians permit to be driven on the public highways. It is interesting to observe that where a person is

[47] Ken Lindup, 'Technology and banking: Lessons from the past', *Digital Evidence and Electronic Signature Law Review* 9 (2012), 91 – 94, https://journals.sas.ac.uk/deeslr/issue/view/309.
[48] For which see the comments of Sir James Munby, President of the Family Division, at [8] in *A and others (Human Fertilisation And Embryology Act 2008)* [2015] EWHC 2602 (Fam) (a further action following on from *AB v CD* [2013] 2 FLR 1357, [2013] EWHC 1418 (Fam)).
[49] As illustrated in the *Bookout* case, for which see *Electronic Evidence*, 6.84, 6.138, 6.155.
[50] The Law Commission, *Evidence in Criminal Proceedings: Hearsay and Related Topics* (1997), 13.13.
[51] See *Electronic Evidence*, chapter 6 for a detailed discussion.
[52] 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.
[53] European Digital Rights highlight the constant failures: https://edri.org/about/.
[54] Bruce Schneier, *Data Is a Toxic Asset*, https://www.schneier.com/blog/archives/2016/03/data_is_a_toxic.html.

killed or injured, the police do not seem to have taken any criminal action against humans – it appears that one merely compensates the family.[55]

On an important note that is discussed in other books in this issue of Book Reports, some lawyers and legal academics support the assertion that software code, in the guise of machines called robots, ought to have a separate legal personality. Professor Russell correctly, in the opinion of this reviewer, suggests that giving legal personality to a machine is absurd (pp 126 – 127).

The text of chapter 10 is positive, but in discussing governance (pp 249 – 253),[56] it is to be wondered whether commercial entities responsible for software will accept the logic of regulation. Professor Russell has probably answered his own question by citing the biologist Paul Berg (p 182), who wrote: 'Once scientists from corporations begin to dominate the research enterprise, it will simply be too late.' At a guess, Professor Russell's suggestions will not be implemented – arguably Professor Zuboff demonstrates the accuracy of this claim, for which see the review above.

Notwithstanding the comments in relation to the legal issues raised in this review, Stuart Russell has written a powerful and important book. The text merely underlines the assertion that judges are now central to the way we live.[57]

[55] Professor Stuart mentions the death of Elaine Herzberg by a vehicle controlled by Uber (p 57) but only provides a media report. The preliminary report of the National Transportation Safety Board is available at https://www.ntsb.gov/news/press-releases/Pages/NR20180320.aspx. It is possible that Rafaela Vasquez, the back-up driver, might be prosecuted, for which see https://www.bbc.co.uk/news/business-50312340. It does not appear that Uber will be the subject of any criminal proceedings, for which see a letter dated 4 March 2019 to this effect written by Sheila Sullivan Polk, Yavapai County Attorney, presently available at https://twitter.com/BiancaBuono/status/1103053274297462784; however, a person driving a Tesla has been prosecuted in Switzerland – this case has only just come to the attention of the editors, and it is anticipated that a translation of the relevant judgment will be published in 2020.

[56] See the comments about governance and Uber mentioned in the review of Charles Morgan, editor, *Responsible AI A Global Policy Framework*, above.

[57] As indicated in 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.