Disclosure and the Common Law Presumption that Computers are Reliable

Peter Bernard Ladkin
20250117: Version 2 of 20250121

The Police and Criminal Evidence Act 1984 (PACE) Section 69[1] read

> ***69 Evidence from Computer Records***
>
> *(1) in any proceedings, a statement in a document produced by a computer shall not be admissible as evidence of any fact stated therein unless it is shown—*
>
> *(a) that there are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer; ,*
>
> *(b) that at all material times the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents ; and*
>
> *(c) that any relevant conditions specified in rules of court under subsection (2) below are satisfied.*
>
> *(2) ………..*

For complex software-based computer systems, clause 69(1)(b) in particular imposed a practically insurmountable burden on users of computer systems and their lawyers, for it is regarded by most software specialists as unrealistic, in the state of the art as it has been and is practiced, to prove the correctness of operation, except in certain branches of the industry in which reliability is paramount and required to be demonstrated in advance by regulation (for example safety-critical avionics for aircraft and SCRAM software in nuclear power stations).

Accordingly, PACE S 69 was considered by the Law Commission in a 1997 report, and repeal was recommended. S 69 was repealed in the Youth Justice and Criminal Evidence Act 1999[2]. The law concerning computer evidence is now given the the common law presumption (hereafter Presumption) that[3]

> *13.13 … … Without section 69, a common law presumption comes into play:In the absence of evidence to the contrary, the courts will presume that mechanical instruments were in order at the material time.*
>
> *13.14 Where a party sought to rely on the presumption, it would not need to lead to evidence that the computer was working properly on the occasion in question unless there was evidence that it may not have been –in which case the party would have to prove that it was (beyond reasonable doubt in the case of the prosecution, and on the balance of probabilities in the case of the defence). ……*

[1] https://www.legislation.gov.uk/ukpga/1984/60/section/69/enacted

[2] https://www.legislation.gov.uk/ukpga/1999/23/contents

[3] The Law Commission, Evidence in Criminal Proceedings: Hearsay and Related Topics (1997), available from https://lawcom.gov.uk/project/evidence-in-criminal-procedings-hearsay/#related

The Presumption was challenged by Stephen Mason, acting for Alain Job, in a case involving ATM Chip&PIN withdrawals before Nottingham Crown Court in 2009 (the judgement, with commentary by Alistair Kelman, has been published[4]) Additionally, the practitioners' handbook[5] Electronic Evidence and Electronic Signatures, edited by Mason and Daniel Seng, has included chapters devoted to the topic since the 2nd Edition in 2010.

I myself and colleagues expert in software reliability have analysed the Presumption in detail and find it wanting[6] We considered this matter because of the Horizon scandal. We and further colleagues have also considered the documentation needed for what I can call here "probity assurance" of computer-based system evidence[7]. Misuse of the Presumption has been highlighted in various Horizon prosecutions (indeed, Marshall et al. (2021) was directly cited in a Nature editorial in January 2024[8] as a result of a television dramatisation of the JFSA struggles with the Post Office, which had aired in early January 2024). However, there were also massive failures of disclosure[9]. As a result, it seems that many people think that the common law Presumption and failures of disclosure are closely linked if not intertwined. Certainly one can envisage a legal strategy to minimise disclosure of computer system failures and other adverse indications of reliability and at the same time to assert according to the Presumption that the computer system was operating correctly.

Indeed, it appears that some people in the judiciary and amongst lawmakers think that the Presumption and disclosure failures are intimately related. For example, in the House of Lords, Lord Camrose (for the Government) replied to Baroness Kidron's proposed amendment to the Data Protection and Digital Information Bill on 24th April 2024, as follows[10]

> *This amendment would require a party relying on computer evidence to provide proof up*

[4] Case Judgement: England and Wales: Job v Halifax PLC, with commentary by Alistair Kelman, Digital Evidence and Electronic Signature Law Review 6 (2009), available from https://journals.sas.ac.uk/deeslr/article/view/1905

[5] Stephen Mason (ed.), Electronic Evidence (2nd edn, LexisNexis Butterworths, 2010). In the current edition, see Chapter 5 of Stephen Mason and Daniel Seng (eds.), Electronic Evidence and Electronic Signatures, Fifth Edition, University of London Press, 2021, available from https://uolpress.co.uk/book/electronic-evidence-and-electronic-signatures/

[6] Ladkin, P.B., Littlewood, B., Thimbleby, H.W., Thomas, M., The Law Commission presumption concerning the reliability of computer evidence, Digital Evidence and Electronic Signature Law Review 17 (2020), available from https://journals.sas.ac.uk/deeslr/article/view/5143

[7] Marshall, P., Christie, J., Ladkin, P.B., Littlewood, B., Mason, S., Newby, M., Rogers, J., Thimbleby, H.W. Thomas, M., Recommendations for the probity of computer evidence, Digital Evidence and Electronic Signature Law Review 18 (2021), available from https://journals.sas.ac.uk/deeslr/article/view/5240 . Also Bohn, N., Christie, J., Ladkin, P.B., Littlewood, B., Marshall, P., Mason, S., Newby, M., Rogers, J., Thimbleby, H.W. Thomas, M., Briefing Note: The legal rule that computers are presumed to be operating correctly – unforeseen and unjust consequences, Digital Evidence and Electronic Signature Law Review 19 (2022), available from https://journals.sas.ac.uk/deeslr/article/view/5476

[8] Anonymous, Computers Make Mistakes and AI will make things worse – the law must recognise that, Editorial, Nature, 23rd January 2024, available at https://www.nature.com/articles/d41586-024-00168-8

[9] Three judges refused applications for relevant disclosure before and during the course of Seema Misra's trial – see footnote 2 to paragraph 5.165 in Stephen Mason and Daniel Seng, editors, Electronic Evidence and Electronic Signatures, Fifth Edition, University of London Press, 2021, available open source at https://uolpress.co.uk/book/electronic-evidence-and-electronic-signatures/. The Williams Inquiry has considered in depth in Phases 5 and 6 in 2024 multiple disclosure failures, such as that of the so-called Clarke Advice, and the Second Sight interim report from 2013, both related to known failures of the Horizon system.

[10] From https://hansard.parliament.uk/lords/2024-04-24/debates/9BA1A8E3-48E3-4472-AF8E-2EFAFC53E605/DataProtectionAndDigitalInformationBill#contribution-B8965FB7-B9C9-41A8-A34B-1637EC154E61

> *front that the computer was operating effectively at the time and that there is no evidence of improper use*[11]*. I and my fellow Ministers .....*
>
> *.. are considering, for example, the way reliability of evidence from the Horizon system was presented, how failures of investigation and disclosure prevented that evidence from being effectively challenged, and the lack of corroborating evidence in many cases. These issues need to be considered carefully, with the full facts in front of us. Sir Wyn Williams is examining in detail the failings that led to the Post Office scandal. These issues are not straightforward. The prosecution of those cases relied on assertions that the Horizon system was accurate and reliable, which the Post Office knew to be wrong. This was supported by expert evidence, which it knew to be misleading. The issue was that the Post Office chose to withhold the fact that the computer evidence itself was wrong.*

The amendment proposed by Baroness Kidron addresses the Presumption; the response on behalf of His Majesty's Government by Lord Camrose recounts exactly the failures of disclosure that occurred in the Horizon scandal.

Whether they are related in any specific incidents such as the Horizon scandal, the two issues are different. Below, I shall give examples in which the Presumption is demonstrably wrong, but all disclosure and fulfilment of the right to inspect were in order.

The rules for disclosure are set out in Rules and Practice Directions Part 31: Disclosure and Inspection of Documents[12]. This defines what a document is:

> *Meaning of document*
>
> ***31.4*** *In this Part –*
> *'document' means anything in which information of any description is recorded; and*
> *'copy', in relation to a document, means anything onto which information recorded in the document has been copied, by whatever means and whether directly or indirectly.*

[11] PBL comment: Whether or not this follows fom Baroness Kidron's proposal, Stephen Mason has pointed out to me that it is not necessary to adduce evidence to prove a computer was operating properly to introduce the evidence into legal proceedings. Where the electronic evidence is disputed, it is however necessary to demonstrate its *authenticity* and *integrity* (for which see Chapter 6 '*Authenticating electronic evidence*' by Luciana Duranti and Allison Stanfield in Mason and Seng, Electronic Evidence and Electronic Signatures. In the Draft Convention on Electronic Evidence Digital Evidence and Electronic Signature Law Review 13 (2016) S1 – S11, https://journals.sas.ac.uk/deeslr/article/view/2321, Article 3 provided for the Agreement on the admissibility of electronic evidence, as follows:
1. Unless otherwise provided in any law operating in the relevant jurisdiction, an electronic record or document may be tendered, subject to the discretion and rules of the court, if the Parties to the proceedings have expressly agreed to its introduction.
2. Notwithstanding the provisions of Article 3(1), an agreement between the Parties on the admissibility of an electronic record or document does not render the record admissible in a criminal proceeding if at the time the agreement was made
(a) the accused person or any of the persons accused in the proceeding was not represented by a lawyer
(b) except where the adjudicator finds that admitting the record or document into evidence does not prejudice the case for the accused.
It follows that it is not necessary to have to provide proof up front that the computer was operating effectively at the time and that there is no evidence of improper use.

[12] https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part31

It defines what the term “disclosure” means:

> *Meaning of disclosure*
>
> ***31.2** A party discloses a document by stating that the document exists or has existed.*

It determines what “standard” documents are to be disclosed:

> *Standard disclosure – what documents are to be disclosed*
>
> ***31.6** Standard disclosure requires a party to disclose only–*
> *(a) the documents on which he relies; and*
> *(b) the documents which –*
> *(i) adversely affect his own case;*
> *(ii) adversely affect another party’s case; or*
> *(iii) support another party’s case; and*
> *(c) the documents which he is required to disclose by a relevant practice direction.*

There is a right (of all parties) to inspect disclosed documents. In the “Volksmund” it is the exercise of this right by a party which is most often referred to as “disclosure” (I prefer to call it “fulfilment of the right to inspect”). Typically, copies of the documents disclosed are also provided to all parties at time of disclosure.

There are examples of incidents in the computer science literature of system unreliability (including deaths) in which, in legal proceedings, all documentation could have been shared (full fulfilment of the right to inspect), but the Presumption would yield an assertion of reliability, whereas the system was in fact in deployment unreliable.

Events with the Therac-25 radiotherapy machine is a well-known example in computer system safety circles[13]. The company that produced the system is a Canadian Crown corporation, Atomic Energy of Canada Limited. The Therac-25 operated in a highly regulated sector, in which the US Food and Drug Administration (FDA) licences medical devices for use and can withdraw a licence and require modification of devices it considers potentially unsafe.

The Therac-25 machine was an evolution of the Therac-20 (and, before that, the Therac-6). The safety properties of the Therac-20, for example inhibiting overdose, were largely hardware-based (for example, interlocks). The Therac-25 transferred some of these features to software.

There were many overdose incidents with the Therac-25. Some of these, but not all, were reported to the FDA, but information about incidents was not being routinely collected and collated

[13] Leveson, N.G., and Turner, C.S., An Investigation of the Therac-25 accidents, IEEE Computer pp18-41, July 1993. A version is available on the Wayback Machine at https://web.archive.org/web/20041128024227/http://www.cs.umd.edu/class/spring2003/cmsc838p/Misc/therac.pdf A modified version of this paper, Leveson, N.G., Medical Devices: The Therac-25, is available at http://sunnyday.mit.edu/papers/therac.pdf . Citations in the text from “Leveson” are to this paper. The Therac-25 case is also discussed in Chapter 5, paragraph 5.181 of Stephen Mason and Daniel Seng (eds.), Electronic Evidence and Electronic Signatures, Fifth Edition, University of London Press, 2021, available from https://uolpress.co.uk/book/electronic-evidence-and-electronic-signatures/

anywhere, and was not necessarily shared with all users, some of whom then went on to suffer similar accidents of their own. The first accident occurred at the Kennestone Regional Oncology Center in Marietta, Georgia. Leveson writes "*Details of this accident …. are sketchy, because it was never investigated.*"[14]

Leveson writes[15]:

> *Inadequate Investigation or Followup on Accident Reports. Every company building safety-critical systems should have audit trails and incident analysis procedures that are applied whenever a hint of a problem is found that might lead to an accident. The first phone call by Tim Still should have led to an extensive investigation of the events at Kennestone. Certainly, learning about the first lawsuit should have triggered an immediate response.*

There are many factors which Leveson and Turner identify as root causes of the incidents, defective documentation and risk analysis amongst them. The point I wish to make is twofold. First, that these accidents occurred, and continued to occur, in a highly regulated environment with specific reporting requirements to the regulator. The question of disclosure and fulfilment of the right to inspect is assured by the regulatory reporting requirements (and also that the manufacturer is a Canadian Crown company with, we may presume, no incentive whatsoever to conceal anything). Second, that had certain documentation existed – had there been a regulatory requirement to collect and collate incidents involving the Therac-25, problems would have been identified sooner and later injuries thereby avoided. Instead, many of those involved, including at the manufacturer, continued to believe that it was not possible to give an overdose with the Therac-25[16].

As the incidents evolved, then, there was no general collocated evidence that the Therac-25 was accident-prone in specific ways. Any general disclosure process would not have uncovered such evidence, since it was not collocated. Were the Presumption to be applied here, it would follow from the Presumption that the Therac-25 was reliable. It wasn't – its operation was very unsafe, as eventually proved to be. Applying the Presumption here would have led to a false assertion. The Presumption leads to false conclusions even where there is no issue with disclosure.

Another example was given in Ladkin et al. (2020)[17], namely the the investigation underlying the Toyota/Bookout civil case, in which a Toyota car was said to have engaged in "unintended acceleration" (that is, the car accelerated even though no command to do so had been given by the driver), which resulted in an accident, injury and death. The amount of work that was put in to demonstrate that such a mode existed in the control software of the car was of the order of many

[14] Leveson, N.G., Medical Devices: The Therac-25, Section 3.1, p9.

[15] Leveson, N.G., Medical Devices: The Therac-25, Section 4, p47.

[16] Many observations in the case descriptions given in Leveson, N.G., Medical Devices: The Therac-25. For example, in Section 3.1, p9: "*It is unclear when AECL learned about [the Kennestone] incident. Tim Still, the Kennestone physicist, called AECL to ask if the Therac-25 could operate in electron mode without scanning to spread the beam. Three days later the engineers at AECL called the physicist back to explain that improper scanning was not possible.*"

[17] Ladkin, P.B., Littlewood, B., Thimbleby, H.W., Thomas, M., The Law Commission presumption concerning the reliability of computer evidence, Digital Evidence and Electronic Signature Law Review 17 (2020), available from https://journals.sas.ac.uk/deeslr/article/view/5143

person years, including a substantial NASA investigation which did not find such a mode. There is no disclosure issue involved – the source code was shared with investigators. The car company maintained a defence for many years that was similar to the Presumption: there is no reason to think there is such a fault in the control software. Until it was finally demonstrated that there was such a fault.

The third example is a generic consideration rather than a specific incident. You cannot present for inspection documentation that does not exist, information that has not been collated. There might well be cases in which not all of the documentation proposed by Marshall et al. (2021)[18] exists. For example if a software-based system has been developed for a client using so-called Agile methods, then documents generally regarded as necessary when development documentation follows the Waterfall model[19], such as a system Functional Requirements Specification, as well as supporting argumentation that the deployed system fulfils this Specification, may not exist. Such a Specification and such argumentation are taken by most software engineers to be essential evidence in assessing system reliability. If they don't exist, any assurance of such reliability is concomitantly weaker. In such a case, requirement for disclosure and fulfilment of the right to inspect can be fully complied with, but the reliability assurance case is nevertheless weaker: less is known about the reliability of the system, not more. This gap in knowledge cannot logically be filled by any legal instrument such as the Presumption. Following the Presumption entails that the absence of critical evidence about reliability, such as in this case, does not weaken the legal argument for system reliability, because the system may be presumed reliable (in the absence of contraindication), which contradicts both the experience and the attitude of most software reliability experts.

There may be reasons other than development lacunae why documentation essential for establishing the reliability of a computer system and thereby the probity of evidence deriving from that system does not exist. A fire may have destroyed important documentation held at a specific location. A disgruntled employee may have used ransomware to encrypt essential electronic documentation.

It goes against the experience of software reliability experts to "presume" anything about the reliability characteristics of a software-based computer system in the absence of pertinent evidence for it; rather, it is for the suppliers, operators and users of the system to establish the reliability characteristics as best they can with whatever documentation exists, and retain any uncertainty about those characteristics engendered by lacking such pertinent evidence. It is surely most appropriate for the law to reflect the experience of such experts, rather than countermand it through the Presumption. This is the point of the recommendations in Marshall et al. (2021)[20].

[18] Marshall, P., Christie, J., Ladkin, P.B., Littlewood, B., Mason, S., Newby, M., Rogers, J., Thimbleby, H.W. Thomas, M., Recommendations for the probity of computer evidence, Digital Evidence and Electronic Signature Law Review 18 (2021), available from https://journals.sas.ac.uk/deeslr/article/view/5240 .

[19] Winston W. Royce, Managing the development of large software systems: concepts and techniques, in Proceedings of IEEE WESCON (1970), available from https://dl.acm.org/doi/10.5555/41765.41801 . Note that nowadays use of the Waterfall model is mostly to establish what system development documentation and relations amongst that documentation there is to be, rather than a guide to how to go about developing a software system.

[20] Marshall, P., Christie, J., Ladkin, P.B., Littlewood, B., Mason, S., Newby, M., Rogers, J., Thimbleby, H.W. Thomas, M., Recommendations for the probity of computer evidence, Digital Evidence and Electronic Signature Law Review 18 (2021), available from https://journals.sas.ac.uk/deeslr/article/view/5240 .

Acknowledgement

PBL is very grateful to Stephen Mason for review, commentary and thereby improvement.