Use of evidence generated by software in criminal proceedings: Call for Evidence by the Ministry of Justice

Submission by James Christie

1) The current common law (rebuttable) presumption is that computers producing evidence were operating correctly at the material time.

(a) Is this presumption fit for purpose in modern criminal prosecutions?

No.

(i) Please specify why you gave this answer.

The presumption was not fit for purpose when it was introduced in 2000. The Law Commission did not understand the nature of complex software systems in the 1990s and misrepresented the submissions of experts it consulted.

In its 1995 consultation paper the Law Commission recommended the repeal of section 69 of the Police and Criminal Evidence Act 1984 and its replacement by;[1]

> *"...the common law presumption that, in the absence of evidence to the contrary, a device of a kind which normally works properly may be assumed to have been working properly at a particular time."*

The Law Commission confirmed this recommendation in its 1997 final report.[2] The wording of the recommendation revealed the Commission's failure to understand computer technology. It is meaningless to talk of complex modern software systems as being "a device". They have myriad hardware and software components, which are changing constantly.

Jason Coyne, the postmasters' expert witness in the Horizon Issues case, asked the Post Office for confirmation of the number of "release notes" (i.e. system changes) between the system's launch in 1999 and 2018. The answer would be startling to people without IT experience.[3]

> *"Post Office have stated that the Horizon system has changed 19,842 times since its inception."*

Such systems require constant, careful management which must be capable of demonstration to auditors. Constant reliability cannot be presumed.

Since 2000 the complexity of software has increased vastly with the prevalence of internet systems. Any processing performed over the internet inevitably requires the use of components that are not under the control of the organisation that owns and manages the system. It is therefore vital that

---

[1] Law Commission, "Evidence in Criminal Proceedings: Hearsay and Related Topics – A Consultation Paper", No 138, (1995). Paragraph XVI.31, page 225.
https://cloud-platform-e218f50a4812967ba1215eaecede923f.s3.amazonaws.com/uploads/sites/30/2016/08/No.138-Criminal-Law-Evidence-in-Criminal-Proceedings-Hearsay-and-Related-Topics-A-Consultation-Paper-1.pdf

[2] Law Commission, "Evidence in Criminal Proceedings: Hearsay and Related Topics", 1997.
https://cloud-platform-e218f50a4812967ba1215eaecede923f.s3.amazonaws.com/uploads/sites/30/2015/03/lc245_Legislating_the_Criminal_Code_Evidence_in_Criminal_Proceedings.pdf

[3] Bates v Post Office Ltd (No 6: Horizon Issues) Rev 1 [2019] EWHC 3408 (QB). Expert Report of Jason Coyne, 16 October 2018. Paragraph 3.8
https://www.postofficetrial.com/2019/06/horizon-trial-jason-coynes-expert.html

system owners can demonstrate that the system was designed and built to detect and handle unexpected behaviour, or the failure, of external components. It is not good enough to assert that the system was built correctly and can henceforward be presumed to be reliable. It is worth stressing the mantra I was taught as an IT auditor.

"Don't tell me – show me."

In recommending the presumption of computer reliability the Law Commission focused on the admissibility of evidence and ignored the experts who urged it to address the issue of reliability. The consultation paper and final report revealed a lack of understanding of the nature of reliability in IT systems.

The Commission failed to understand the importance of the distinction between hardware, which is generally reliable, and software, which is of widely varying quality. It also did not consider the reliability of data, as distinct from that of hardware and software. I examined these failings in a 2023 article in the Digital Evidence and Electronic Signature Law Review.[4]

(b) How easy or difficult do you believe it is at present for this presumption to be effectively rebutted?

It is impossible to rebut the presumption unless the provider of computer evidence co-operates in a way that weakens their case. That is unrealistic, as I shall explain in the next section.

(c) What barriers do you see in effectively rebutting this presumption?

(i) Please give examples where possible.

Rebutting the presumption requires full disclosure of information that would weaken the case of the evidence supplier. For disclosure to be effective there must not only be full willingness to co-operate, but also responsible and competent management of both the development and running of the system. There must be detailed records kept of test results, relevant audits, bugs, and fixes.

In my experience incompetent organisations will not even be aware that they should retain this information to demonstrate that they are in control of their systems. It is therefore likely, under the current arrangements, that organisations will provide unreliable evidence along with honest, but mistaken, assurances that they know of no relevant problems.

This creates a paradox that undermines the presumption, and the Law Commission's naive complacency about rebuttal.

Rebuttal is straightforward only if the supplier of evidence maintains high professional standards. It is almost impossible if the supplier is incompetent and irresponsible. Rebuttal is therefore only possible, in theory, if the evidence comes from a reliable source, in which case the attempt at rebuttal should fail. Rebuttal is likely to be impossible if the source is unreliable, because the supplier of evidence is too incompetent to hold the relevant information. Unreliable evidence, from incompetent providers, therefore evades rebuttal and is taken at face value, (see the Post Office scandal).

[4] James Christie, "The Law Commission and section 69 of the Police and Criminal Evidence Act 1984", 20 Digital Evidence & Electronic Signature Law Review (2023).
https://journals.sas.ac.uk/deeslr/article/view/5642

If defence counsels challenge the evidence they will be asked for specific information about how the system has produced inaccurate results, or they will be accused of conducting "fishing expeditions".[5]

This raises another aspect of the Law Commission's poor understanding of complex software systems. The Commission stated in paragraph 13.7 of its 1997 report that;

> *"...section 69 fails to address the major causes of inaccuracy in computer evidence. As Professor Tapper has pointed out, 'most computer error is either immediately detectable or results from error in the data entered into the machine'."*

Firstly, serious errors can be invisible to end users. They might arise from back-end batch processing (i.e. programs processing large volumes of data from multiple users after end-users have submitted their data), communications failures, or any number of problems that are not apparent to the user sitting at a keyboard and terminal.

Even technical experts face great difficulty in assessing whether complex computer systems are performing reliably and accurately. Mistakes in processing are often very hard to detect. This is beyond the ability of non-technical users, even if they have sufficient system access, and no well managed organisation would permit end users that level of deep access.

If errors are "immediately detectable" then they are unlikely to be the problems that trouble courts. They will not be the errors that lead to expensive, damaging litigation, or that might result in erroneous or unreliable evidence being given in criminal prosecutions.

The Post Office Horizon Issues trial in 2019 highlighted a Horizon error, the "receipts and payments mismatch" bug[6], which resulted in Post Office branch users being told their account was in balance when the central system recorded a discrepancy for which users were liable. Such an error was impossible for users to detect. Justice Fraser identified this is a problem for the whole Horizon system.

> *"1000: Because the reports and data available to SPMs were so limited, their ability to investigate was itself similarly limited. The expert agreement to which I refer at [998] above makes it clear in IT terms (based on the transaction data and reporting functions available to SPMs) that SPMs simply could not identify apparent or alleged discrepancies and shortfalls, their causes, nor access or properly identify transactions recorded on Horizon, themselves. They required the co-operation of the Post Office."*[7]

A second problem with the Law Commission's use of Professor Tapper's quote is that it was lifted out of context. Professor Tapper was offering a comment that was in the nature of an obiter dictum. It was not material to the main argument of the article in which it appears. He was referring to section 5 of the Civil Evidence Act 1968 which concerned the admissibility of computer evidence in civil proceedings. i.e. the civil law equivalent of PACE 1984 section 69. The full passage criticised civil legislation as being too lax because it permitted the use of computer records where the person who input the information could not vouch for its truth.

---

[5] See Paul Marshall et al, "Recommendations for the probity of computer evidence". Digital Evidence & Electronic Signature Law Review, 18 (2021). Page 21.
https://journals.sas.ac.uk/deeslr/article/view/5240

[6] Bates v Post Office Ltd (No 6: Horizon Issues) Rev 1 [2019] EWHC 3408 (QB). Paragraphs 427-434.
https://www.bailii.org/ew/cases/EWHC/QB/2019/3408.html

[7] Bates v Post Office Ltd (No 6: Horizon Issues). Paragraph 1000.

> *"The most surprising feature of section 5 is that it makes no requirement that the originator of the information processed by the computer should have had, or even be reasonably capable of being supposed to have had, personal knowledge of the truth of that information. This seems quite extraordinarily lax, given that most computer error is either immediately detectable or results from error in the data entered into the machine. So widely has this been accepted that it has become institutionalized into the acronym 'GIGO,' or 'garbage in, garbage out'."* [8]

It was a remarkable decision of the Law Commission to take an argument criticising lax admissibility of computer evidence in civil cases to justify more liberal admissibility of computer evidence in criminal cases.

Professor Tapper's article was the only source provided by the Law Commission to justify its assertion that section 69 "fails to address the major causes of inaccuracy in computer evidence". The professor was clearly misrepresented, as I argued in my 2023 article "The Law Commission and section 69 of the Police and Criminal Evidence Act 1984".[9]

Any practitioner with experience of working with complex software systems knows that the Law Commission was mistaken about the causes of inaccuracy, and the ease with which they can be detected. This misunderstanding undermines the justification for the presumption that computer evidence should be considered reliable. Rebuttal, to the standard required by courts, is almost impossible in practice.

The prosecution of Seema Misra (Regina v Seema Misra, T20090070, 2010) provides a tragic example of how difficult it is to rebut the presumption. The prosecuting barrister, Warwick Tatford, in his opening and closing speeches made heavy emphasis of the assertion that system problems are obvious to users.[10]

> *"The whole point of... any computer problem is that the operators can see something is going wrong. They are not going to know what the problem is, what the cause of the problem is, but they are going to see that something is going wrong, and if something is going wrong with the computer they will phone the Fujitsu helpline."*

When Mr Tatford appeared before the Post Office Horizon IT Inquiry he was questioned by Edward Henry KC, counsel for postmasters, about his argument about the ease with which problems can be spotted.[11]

> *"Could it have been that the theme that such flaws would have been obvious to the user was a strategy to convince the judge... and the jury... that Mrs Misra should have been keenly aware of any Horizon problems, that she should have been able to discern and diagnose bugs, errors and defects?...*

---

[8] Professor Colin Tapper, "Discovery in Modern Times: A Voyage around the Common Law World", 67 Chi.-Kent L. Rev. (1991). Page 248.
https://scholarship.kentlaw.iit.edu/cklawreview/vol67/iss1/8/

[9] James Christie, "The Law Commission and section 69 of the Police and Criminal Evidence Act 1984". Digital Evidence & Electronic Signature Law Review, 20 (2023).
https://journals.sas.ac.uk/deeslr/article/view/5642

[10] Case Transcript - Regina v Seema Misra, T20090070 Day 7 Tuesday 19 October 2010. Pages 24-25.
https://journals.sas.ac.uk/deeslr/article/view/2198

[11] Post Office Horizon IT Inquiry. Phase 4 - 15 November 2023. Evidence from Warwick Tatford (external counsel instructed in the prosecutions brought against Carl Page and Seema Misra).
https://www.postofficehorizoninquiry.org.uk/hearings/phase-4-15-november-2023

> *Do you also think that framing the issue in that way was to reverse the burden of proof because, of course, in law, it was the Post Office's duty, prosecuting the case in the name of the Crown, to prove that the system was working, to satisfy the jury that they were sure that the system was working. It was not for Mrs Misra to identify when it may not have been?"*

The point is crucial. If one assumes that errors are obvious then the effect is to reverse the burden of proof. This assumption about errors underpins the flawed presumption of computer reliability.

This failure amongst the legal profession to understand computer technology and the concept of reliability in complex software systems has led to further problems in the application of the presumption. Lawyers often struggle to use statistical analysis correctly in their assessment of whether computer evidence should be considered reliable.

This was exemplified in Seema Misra's prosecution. Warwick Tatford made this argument in his opening speech.[12]

> *"The computer system quite literally will process millions of transactions every single day and in peak times like around Christmas perhaps nearly 20 million transactions per day.*
>
> *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...*
>
> *Not only is this a robust system that was used every day, you are also going to hear evidence from the person who until very recently was running West Byfleet, a Mr Vasarmy. He took over the post office after Mrs Misra and he is going to tell you that he has not had a problem with the computer system. It is the same system. Nothing has changed. He has not had a problem."*

The passage was worth quoting at length because of the way it combines four fallacies. Firstly, as I have already argued, it is a fallacy to assume that system errors are always visible to users.

In addition to this mistake, Tatford's argument contained a serious statistical fallacy. Even if a massive, complex, distributed system that was operating across the country with potentially fragile connections was *generally* reliable it is fallacious to argue that it was therefore *necessarily* accurate in the case in question. As was pointed out by Jason Beer KC (Counsel to the Inquiry) and Edward Henry KC in the session of questioning Mr Tatford (referred to above) at the Post Office Horizon Inquiry, the argument was a variation on the Prosecutor's Fallacy.[13] This fallacy confuses two probabilities; the probability that a bug will randomly produce a discrepancy at a specific location

---

[12] Case Transcript - Regina v Seema Misra, T20090070 Day 1 Monday 11 October 2010. Pages 49-50. https://journals.sas.ac.uk/deeslr/article/view/2198

[13] Kathy Taylor. "The Prosecutor's Fallacy". Centre for Evidence-Based Medicine, Nuffield Department of Primary Care Health Sciences, University of Oxford (2018). https://www.cebm.ox.ac.uk/news/views/the-prosecutors-fallacy

Phase 4 - 15 November 2023. Evidence from Warwick Tatford (external counsel instructed in the prosecutions brought against Carl Page and Seema Misra). https://www.postofficehorizoninquiry.org.uk/hearings/phase-4-15-november-2023

and time, and the probability that a bug was the cause if a discrepancy occurs. These two probabilities have very different values. I shall return to that point in the section covering proposed solutions.

There were two further fallacies in Warwick Tatford's line of argument. The third fallacy is the belief that a system like Horizon remains *"the same system"* over time and will work the same way for all users. Such systems change constantly, and will behave differently at different times. Even if the system has not changed it is possible that different, legitimate actions by different users who are performing the same tasks will produce different results, some of which might be the result of bugs.

The Dalmellington bug, referred to in the Horizon issues case, is an example.[14] If a user pressed 'enter' a second time when the screen froze a second transaction would be recorded, with serious financial consequences. Users might not have been *supposed* to hit enter, but for some users it was a natural response to a system problem. Software has to be designed to cope with unpredictable users and a presumption that it is either working or not working is misconceived.

While discussing the Receipts and Payments Mismatch bug (see above) Justice Fraser noted that it was fallacious of the Post Office's to assertion that it was not a true bug because it would require "an unusual sequence of events". The system should have been designed to cope with what was a reasonable and predictable action by a user.

> *"136. I do not accept that this was a particularly unusual sequence. If there was a discrepancy, I do not see why it is suggested it would be unusual for a SPM to decide to cancel the rollover. This is, in my judgment, something which could be expected to happen sometimes, and plainly the absence of any message to the user could potentially contribute to this."*[15]

The fourth fallacy was related to the earlier point about errors being readily visible. Bugs might remain undetected within systems for years. These are latent bugs. In a huge study in the 1980s Ernest Adams found that;[16]

> *"...lots of software faults took more than 5,000 operating years to be revealed. He found that more than 90% of faults in the software would take longer than 50 years to become failures."*
>
> NB An operating year is the equivalent of one computer running for one year.

The study looked at IBM mainframe operating systems. This is the massively complex technical software which serves as the foundation on which business application systems are built. Application systems must be built to cope with the possibility of underlying technical problems, and to cope

---

[14] Bates v Post Office Ltd (No 6: Horizon Issues) Rev 1 [2019] EWHC 3408 (QB), [427]-[434].
https://www.bailii.org/ew/cases/EWHC/QB/2019/3408.html
A brief, simpler account of the Dalmellington Bug is available here.
Alex Hern, "How the Post Office's Horizon system failed: a technical breakdown". Guardian, (2024).
https://www.theguardian.com/uk-news/2024/jan/09/how-the-post-offices-horizon-system-failed-a-technical-breakdown

[15] Bates v Post Office Ltd (No 6: Horizon Issues), 'Technical Appendix to Judgment (No.6) "Horizon Issues". Paragraphs 134-136.
https://www.judiciary.uk/wp-content/uploads/2022/07/bates-v-post-office-appendix-1-1.pdf

[16] Original source: Edward N Adams, "Optimizing Preventive Service of Software Products" IBM Journal of Research and Development, Vol 28, Iss. 1 (1984).
Via Simon di Nucci, "Updating Legal Presumptions for Computer Reliability", The Safety Artisan (2024).
https://www.safetyartisan.com/2024/08/07/updating-legal-presumptions-for-computer-reliability/

with unexpected latent bugs emerging long after launch. It is always dangerous to assume that a lack of error emerging in the past guarantees reliability in the future.

A simple coding error might not manifest itself for a long time. Latent bugs can lurk undetected within systems for years before they are exposed by the system's inability to handle changed circumstances, or by user actions that the system designers never anticipated. Such novel user behaviour might be entirely innocent and responsible, and it is disingenuous (at best) for this to be classed as illegitimate because it exposed a bug.

In the technical appendix to the Post Office Horizon Issues case Justice Fraser commented on the concept of user error bias;

> *"...where people in IT constantly blame the user when actually it is not their fault...*
>
> *...In my judgment – and regardless of whether Fujitsu and/or the Post Office was applying user error bias, or not – it is clear to me that Fujitsu was far too ready, even after investigations that clearly included the express discovery of bugs in code, to ascribe possible user error to the effect of bugs, errors and defects that caused impact to branch accounts."*[17]

This tendency highlights a further problem with the presumption of computer reliability and the assumption that it would be readily rebuttable. In practice the various problems with the presumption, and the low level of technical knowledge in the legal profession, place an impossible burden on the party wishing to rebut the presumption that computer evidence is reliable.

The difficulties imposed on the party that wishes to rebut the presumption of reliability mean that deep technical expertise is required. If defendants are to receive a fair trial they must have access to such expertise. That provide impossible for Tracy Felstead, one of the Post Office Horizon victims, as Paul Marshall, her defence counsel, explained.

> *"In the course of her prosecution, a technically skilled expert was instructed on her behalf. His name is Michael Turner. I have spoken with him. He is very experienced. I have seen the detailed request for disclosure he prepared and provided to Fujitsu and the Post Office that, remarkably, he still retains. The response of the Post Office to his requests, at a meeting, was to ask who was expected to pay for the Horizon disclosure he wanted to see? It was suggested that it would cost £20,000 to produce. Mr Turner was not called at Tracy's trial. In 2002 Tracy was convicted and imprisoned in Holloway women's prison. She was 19 years' old."*

Tracy Felstead could not afford to pay £20,000 to rebut the presumption and secure a fair trial. Her experience was not unique. Researchers reported in 2023 that difficulties in obtaining legal aid to commission experts who can examine computer evidence in England and Wales was making it increasingly difficult for defence teams to represent defendants effectively.[18]

> *"... providing forensic expertise for a defendant relies on the ability of the defence team to secure the legal aid funding necessary to commission expert service and the timeliness of*

[17] Bates v Post Office Ltd (No 6: Horizon Issues), Technical Appendix. Paragraphs 451-452.

[18] Dana Wilson-Kovacs, Rebecca Helm, Beth Grown, Lauren Redfern, "Digital evidence in defence practice: Prevalence, challenges and expertise", The International Journal of Evidence & Proof (2023), Vol. 27(3). Page 238.
https://journals.sagepub.com/doi/10.1177/13657127231171620

their application. This process is subject to competitive bidding, with teams having to submit three expert quotes to the Legal Aid Authority (LAA), detailing the work required. However, the low expert payment rates and "demobilising [sic – original source says 'demoralizing'] interactions with the LAA" (Welsh and Clarke, 2021: 468[9]) have led defence lawyers and expert witnesses to query the quality of casework provided, to question the long-term sustainability of the criminal defence profession and to highlight the increase in the risk of miscarriages of justice."

If the presumption is retained that computer evidence is reliable then further miscarriages of justice are inevitable. In practice reliance on rebuttal is impractical and almost always impossible. That is how the presumption operates. That is why it should be replaced by a mechanism that recognises the nature of complex IT systems and the difficulties of working with them responsibly.

2) Are you able to provide examples from other jurisdictions or situations where the reliability of software must be certified?:

a) As examples of good practice?

b) As examples of things to be aware of?

I am aware of other jurisdictions that either require certification of evidence, or set a baseline that providers must meet. However, commenting on the effectiveness of these procedures in those contexts is outside my area of expertise.

It would be worth consulting the safety critical profession to learn what practices are more widely applicable. Too many IT developers take a casual approach to the quality of their work. The safety critical experts know that people will die if they are careless. The submission by Alistair Kelman and myself to this consultation mentions this.

3) If the position were to be amended, what in your opinion would be the most appropriate and practicable solution given our aims and objectives set out above? It would be helpful if your answer could address as many of the below as possible:

I have worked on two different proposals over the last few years; a joint proposal with legal, academic and IT experts who are concerned about the current position, and a proposal initiated by Alistair Kelman, which he has submitted to this consultation.

The first proposal, "Recommendations for the probity of computer evidence" [20] (henceforward Marshall et al), argues that that new approach should involve two stages. The first stage would require providers of evidence to show the court that they have developed and managed their systems responsibly, If they have been responsible then it will be straightforward to demonstrate that. They will have the documents and reports on hand. These should include known bugs, the relevant security standards and processes, the results of relevant IT audits, change and problem

[1919] Lucy Welsh, Amy Clarke, "United by cuts: exploring the symmetry between how lawyers and expert witnesses experience funding cuts (Version 1)". University of Sussex, (2022). Page 468. https://hdl.handle.net/10779/uos.23489345.v1

[20] Paul Marshall, James Christie, Peter Bernard Ladkin, Bev Littlewood, Stephen Mason, Martin Newby, Jonathan Rogers, Harold Thimbleby and Martyn Thomas CBE. "Recommendations for the probity of computer evidence". Digital Evidence & Electronic Signature Law Review, 18 (2021). https://journals.sas.ac.uk/deeslr/article/view/5240

records, and evidence appropriate measures have been taken to prevent unauthorised amendment or deletion of data.

If providers of evidence cannot demonstrate that their system development and management practices have been responsible, or if there are bugs relevant to the evidence given to the court, or there are a large number of bugs, then there should be a second stage. The onus would then be on the provider of evidence to show the court why none of these failings or problems affect the quality of evidence, and why it should still be considered reliable.

The second proposal, by Alistair Kelman and myself, has been submitted separately to the Ministry of Justice as part of this consultation, "A Statutory provision to implement Bayesian Analysis in computer records"[21] (henceforward Kelman-Christie). This would stipulate that 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;

i) that a Bayesian Analysis of all the risk factors that could lead to the statement being inaccurate are below a probability threshold, which would be set by Parliament.

ii) In cases where the Bayesian Analysis is below the probability threshold then the judge would have a discretion to admit the statement as evidence after a voir dire hearing on the admissibility of the evidence.

iii) In cases where the Bayesian Analysis is below the threshold then any Directors' and Officers' Policy (i.e. management liability insurance) protecting Directors and Officers of the company providing the computer evidence would be void.

The Bayesian approach is intended to reduce the risk of prosecutors applying the flawed statistical logic we saw from Warwick Tatford in the Seema Misra trial. It is vital when evaluating evidence that courts can distinguish between the probability that an action will occur and produce a specific outcome, and the probability that if the outcome is detected then that action was the cause. This is the essence of the Prosecutor's Fallacy (referred to earlier).

This Kelman-Christie submission also argues that providers of computer evidence should be expected to demonstrate how they have built and managed software to reduce the risk of their systems straying beyond the margins of acceptable behaviour into the extremes where accidents can happen and unreliable evidence might be produced.

If IT systems are to produce evidence that can be relied on in criminal prosecutions then they must be built to a higher standard than if the system's purpose is routine administration of the business.

One of the serious failings in the Post Office Horizon scandal was the implicit assumption, accepted by Fujitsu, the Post Office, and prosecutors, that if a system was considered reliable for one purpose, then it could be considered reliable for all purposes. It is impossible to assess the reliability of a

[21] Alistair Kelman and James Christie, "A Submission to the Open call for evidence: Use of evidence generated by software in criminal proceedings". (Section "A Statutory provision to implement Bayesian Analysis in computer records"). Submission to the Ministry of Justice, April 2025. https://clarotesting.wordpress.com/wp-content/uploads/2025/04/use-of-evidence-generated-by-software-in-criminal-proceedings-alistair-kelman-and-james-christie-v2-jdc-final-1-1.pdf

system unless one is clear about the purpose. That is a basic principle of IT audits intended to assess the "processing integrity" of computer systems.[22]

a) What procedural safeguards need to be in place to ensure your proposed solution is effective?

The question of procedural safeguards is more of a legal matter than a technical one. I am not qualified to comment on this.

b) How might we ensure that any proposed solution is, as far as is reasonable possible, future-proofed?

There can be no guaranteed future proofing in IT. However, reasonable steps can be taken to reduce the risk. Any solution should avoid overly prescriptive rules about the exact form that compliance should take. It should be based on clear principles to reduce the risk that advances in technology or changes in practice will render the solution obsolete and requiring frequent change.

Good examples of relevant principle-based standards are those of the Institute of Internal Auditors,[23] and the IT audit models defined by the American Institute of Certified Public Accountants (AICPA).[24] It is possible to comply with some over-prescriptive rules-based standards by concentrating on the means and ignoring the purpose of the standard. That is impossible with clear, principle-based standards like those set by the IIA and AICPA.

The rapid advances and spread of artificial intelligence, and also quantum computing, present troubling challenges to traditional ideals of transparency and accountability. The presumption of reliability was always detached from the reality of conventional computing. The presumption is therefore even more irrelevant and indeed more likely to produce unjust outcomes if courts are dealing with artificial intelligence and quantum computing.

If builders of such systems cannot comply with fundamental principles of transparency and auditability they should not expect courts to place reliance on them without strong supporting evidence. Such systems should be built in a way that allows humans to assess how and whether they have produced the right answer. This will entail probabilistic judgments rather than binary decisions that a system is either reliable or unreliable. The two proposals on which I have worked would handle this issue better than the current arrangements.

c) How might we ensure that any proposed solution is operationally practical?

Both proposals, Marshall et al and Kelman-Christie, are based on the reasonable assumption that there should be a baseline level of competence and responsibility expected from providers of evidence. Suppliers of evidence who meet this baseline will have produced secondary, supporting evidence because they need it to show that they are in control of their systems, as is expected by regulators, auditors, and corporate governance professionals. There should not be a great deal of

[22] See James Christie, "The Post Office IT scandal – why IT audit is essential for effective corporate governance", Digital Evidence & Electronic Signature Law Review, 19 (2022), page 30. https://journals.sas.ac.uk/deeslr/article/view/5425

[23] "International Standards for the Professional Practice of Internal Auditing", Institute of Internal Auditors (2017). https://www.theiia.org/en/standards/what-are-the-standards/mandatory-guidance/standards/

[24] The detail of the AICPA's audit models is behind a paywall. See my article on the role of IT audit in corporate governance for an overview.
James Christie, "The Post Office IT scandal – why IT audit is essential for effective corporate governance", pages 24-28.

additional work to produce secondary, supporting evidence for responsible providers of computer evidence.

It is therefore important that the criteria for acceptable evidence are aligned with professional good practice. This should cover IT and engineering bodies, such as the British Computer Society (BCS), and also those with experience in inspecting and assessing complex software systems. In particular the Institute of Internal Auditors (IIA), and ISACA (formerly the Information Systems Audit and Control Association) should be consulted.

The BCS has already stated that it supports replacement of the presumption. Sam de Silva, chairperson of the BCS's Law Specialist Group, has set out the BCS's position.

> *"Organisations relying on evidence generated from computer systems to support prosecutions should be required to prove that the underlying computer system is reliable."*[25]

Both proposals would need some form of expert who is independent of the evidence supplier. Dr Stephen Castell has argued for the appointment of Independent Technical Assessor to guide the courts.[26]

> *"Over many years, I have published extensively on the questionable presumption of the reliability of computer evidence, beginning with work commissioned by HM Treasury on the admissibility of computer evidence in court and the legal admissibility, reliability and security of IT systems. Published in 1990 by permission of HMG, that work was definitive in the critical field of the legal standing and trustworthiness of computer software and systems, and of electronic evidence derived from such systems. My recommendations included that, in court trials where computer evidence is to be adduced, there should be appointed an Independent Technical Assessor to assist the Judge."*

It is worth noting that Dr Castell was referring to the same recommendation, in more detailed form, that he made in his 1990 Appeal Report,[27] which the Law Commission quoted to justify the recommendation to repeal PACE 1984 section 69 without replacement in its 1995 consultation paper. Dr Castell, in the Appeal Report, had in fact stressed that repeal should be accompanied by measures to ensure that providers of computer systems must be required to demonstrate reliability. The Law Commission did not explain why it quoted Dr Castell in such a selective and misleading manner.

d) If your proposed solution requires the use of expert witnesses (either jointly or singly instructed), what expertise and qualifications would that person require? To your knowledge are there sufficient such people at present?

---

[25] "'Computer is always right law' must be urgently reviewed to stop another Post Office scandal, says professional body".British Computer Society (2024). https://www.bcs.org/articles-opinion-and-research/computer-is-always-right-law-must-be-urgently-reviewed-to-stop-another-post-office-scandal-says-professional-body/

[26] Dr Stephen Castell, "Computer Evidence: presume nothing, trust no software or data, engage an expert. Costly? Just look at the cost if you don't", The Barrister, (2023). https://barristermagazine.com/computer-evidence-presume-nothing-trust-no-software-or-data-engage-an-expert-costly-just-look-at-the-cost-if-you-dont/

[27] The VERDICT Report was written in 1987. It was government confidential (and classified). The government later allowed it to be published, in edited/sanitized form, as follows.
Dr Stephen Castell, "The Appeal Report", Eclipse Publications, (1990) ISBN 1-870771-03-6).

Either of the proposed solutions on which I have worked would require some expert witnesses in some form. I do not feel qualified to express a detailed opinion on the level of expertise required. I refer readers to the submissions made by Dr Peter Bernard Ladkin and Professor Harold Thimbleby to the consultation.

4) In your opinion, how should 'computer evidence' for these purposes be best defined?

a) Do you agree that evidence generated by software, as set out above, should be in scope, and that evidence which is merely captured / recorded by a device should be out of scope? Please provide a rationale for your answer.

i) Can you provide specific examples of the type of evidence you believe should be in scope?

ii) Can you provide specific examples of the type of evidence you believe should be out of scope?

My concern is mainly about the quality of evidence produced by large software systems with multiple component, such as Horizon, and this is also the focus of the Ministry of Justice's consultation. However, if single devices, which are simpler in relative terms, are excluded that risks perpetuating the fundamental error of the Law Commission in recommending the introduction of the presumption.

Such communications devices are not simple and mechanical in the way that the law currently assumes all IT equipment and systems to be. They depend on complicated software. Extraction and analysis requires great care. It should not be presumed that this has been done properly. There should be supporting secondary evidence.

The same applies to extraction and analysis of data from the sort of large systems that are within the consultation's scope. "Computer evidence" should be defined so that it includes the extraction and analysis of data, not just the original data in the source system.

When I worked on fraud investigations I routinely extracted and analysed data from live systems. The output we held as evidence was never simply the final report, but a full package showing how the report had been compiled. This would consist of the JCL (IBM Job Control Language) showing which versions of which files were input to the analysis, the successive processing steps and the results of each stage, the full set of computer code for my analysis, and the resulting report. The full paper packages on single, continuous, paper listings were handed over to the police.

It was therefore possible for the whole exercise to be scrutinised and recreated from the source data by an independent expert if our evidence were challenged. That seems a reasonable standard of minimum good practice.

5) Are there any other factors which you believe are important for us to consider?

Two important lessons should be learned from the Post Office scandal about reliance on technical experts, and the current level of technical expertise in the legal profession.

Firstly, lawyers and judges must be aware of the need to call in technical experts. Too often courts cases have been conducted as ill-informed debate between skilled barristers in front of a judge who is usually no wiser. Juries are therefore presented with inaccuracies, in varying degrees, and

statistical nonsense. It should not be the sole responsibility of the defence to call in expert witnesses who can shed a light on what has happened for the benefit of juries. All parties need some form of guidance to help them avoid errors that are obviously egregious to practitioners. Lawyers need the humility to know when they should defer to experts from other fields.

A linked secondary point is that there is clearly a lack of technical knowledge and understanding in the legal profession. A thorough, modern, legal education requires a better understanding of technology. Without a basic grasp of the nature of modern IT lawyers will not grasp the limits of their knowledge. One needs a grounding in order to understand which experts to call in, and when they are required. Studying the Post Office scandal, and the background, has shown me that many lawyers, even distinguished ones, lack the knowledge to understand the extent of their ignorance about computers. That will have to change.

I urge readers, especially lawyers, to refer to the text book edited by Stephen Mason and Daniel Seng, "Electronic Evidence and Electronic Signatures" [28]. This is in its 5th edition but sadly has had little impact within the legal profession.

A final plea is for there to be more communication and contact between lawyers and IT practitioners. The current presumption that computer evidence should be considered reliable is regarded as preposterous by practitioners, most of whom I believe to be unaware that it even exists. If the legal profession had been aware earlier of the deep scepticism that IT experts have about the presumption then I doubt if it would ever have been introduced.

Would we have any legal presumption about medical matters that doctors were convinced was based on a misunderstanding of how the human body worked?

James Christie, 10 April 2025

[28] Stephen Maso & Daniel Seng (editors), "Electronic Evidence & Electronic Signature" 5th edition, Institute of Advanced Legal Studies, (2021).
https://uolpress.co.uk/book/electronic-evidence-and-electronic-signatures/