The use of evidence generated by software in criminal proceedings

Submission dated 14 April 2025

Stephen Mason

1. This submission is in response to the Ministry of Justice call for evidence that began on 21 January 2025 and will end on 15 April 2025.
2. The Ministry of Justice are concerned about the current common law (rebuttable) presumption that computers producing evidence were operating correctly at the material time.
3. I have had the advantage of reading in advance the submission of Professor Peter Sommer, the joint submission by Alistair Kelman and James Christie,[1] and the separate submission by James Christie. These submissions are important to this call for evidence. I have not replicated the detailed discussions contained in these submissions.

Preliminary observation

4. In 1995-1997, the Law Commission committed the error of basing their recommendation on basic breath alcohol analysis testing devices. Computers and computer systems had manifestly become more complex and sophisticated by the last two decades of the twentieth century, which meant that such a narrow focus was mistaken. As indicated by Professor Peter Sommer, this call for evidence appears to be predicated on a single large computer system that produces computer output. The questions asked in this call for evidence appear to repeat the earlier error and fail to grasp the magnitude, range, and complexity of the contemporary software environment.

The need for the authentication of electronic evidence

5. Our reliance on output from electronic devices as evidence is complete and unremarkable. Electronic evidence is inherently complex and diverse, encompassing outputs from digital devices, communication systems, and software-driven processes. The sophistication of modern software systems introduces significant challenges because errors or bugs may remain undetected yet profoundly distort outcomes. For instance, software defects can cause systems to deviate from intended behaviour, leading to catastrophic consequences in a legal context.[2] Moreover, electronic evidence often involves layered dependencies, where the reliability of one component affects another.
6. The Post Office Horizon IT scandal exemplifies these risks. The system erroneously reported financial discrepancies, resulting in wrongful prosecutions of subpostmasters and subpostmistresses. To adopt the analysis by Professor Daniel Seng in an e-mail to me,[3]

---

[1] Although I am not sure that the inclusion of Bayes law in this context will be helpful.

[2] For an analysis of the decision of the Court of Appeal in the appeal of the subpostmaster David Cameron, (*White v Post Office Ltd* [2022] EWCA Crim 435, https://www.bailii.org/ew/cases/EWCA/Crim/2022/435.html, see Peter Bernard Ladkin, Stephen Mason and Harold Thimbleby 'Misunderstanding Digital-Computer Technology in Court: A Commentary', 21 *Digital Evidence and Electronic Signature Law Review* (2024), 1-13, https://journals.sas.ac.uk/deeslr/article/view/5776/5406.

[3] I am indebted to Professor Daniel Seng for kindly taking time out of a very busy schedule for reviewing a previous iteration of this submission. I also thank Peter Bernard Ladkin, Professor i.R. of Computer Networks and Distributed Systems at Bielefeld University, and Martyn Thomas CBE, Emeritus Professor, Gresham College, London; Visiting Professor of Software Engineering at Aberystwyth University, Wales.

the back-end records used as a basis for the prosecutions against the subpostmasters and subpostmistresses were unreliable because of a multiplicity of software defects when the front-end systems transmitted the transactions data for back-end processing. This scandal underscores the critical need to authenticate electronic evidence rigorously.

7. Authentication thus requires that the proponent of such data verify that the data is genuine and unaltered, and accurately reflects the claimed source. It follows that the burden must fall on the party introducing such evidence to prove its authenticity, bringing it into line with principles applied to traditional forms of evidence.

8. Where forensic tools are used to extract electronic evidence – such as smartphone data – this should entail the validation of both the software and the electronic evidence that it outputs, because such tools are themselves prone to errors.[4]

The role played by the presumption in legal proceedings

9. The common law presumption, rooted in historical analogies to mechanical instruments, assumes that systems function correctly at the material time.[5] It serves as an expediency mechanism, to streamline the process for tendering such evidence in legal proceedings. The proper application of the presumption must be that it only applies to the class of instruments for which judicial notice has been taken that they are generally trustworthy and have functioned reliably when producing the evidence that is sought to be admitted. It is debatable whether such classes of instruments should continue to be given such a benefit, given that they are also, in the main, now controlled by software. It was never intended to be used for a carte blanche admission of all forms of electronic evidence, because there is no accepted presumption among technologists and computer scientists that all software processes are reliable.

10. Where the presumption is indiscriminately applied to software, this must be fundamentally flawed.[6] The same presumption has never been applied universally to recordings and measurements made from all mechanical instruments.

---

[4] Extraction reports from mobile telephones (and smartphones, more importantly) will rely on the accuracy or otherwise of the software used to extract the data. In follows that the software used to extract the data should be authenticated. Forensic software is also prone to bugs and errors, and this must not be discounted. For a brief introduction to the problems of forensic tools, see Mason and Seng, 9.69-9.92. Note also that this is 'demonstrative evidence' and is not true evidence, for which see Daniel Kiat Boon Seng, "'To Admit or Not to Admit': That is the Question for AI Evidence" in Ho Hock Lai and Kelvin F K Low (eds), *A Gentleman of the Law: Essays in Honour of Tan Yock Lin* (NUS Press, forthcoming), https://ssrn.com/abstract=5184567.

[5] Beginning with the second edition of *Electronic Evidence* (2010), I set out to demonstrate that the presumption was false. This research began as a direct result of the case of *Job v Halifax PLC* (not reported) Case number 7BQ00307, 6 *Digital Evidence and Electronic Signature Law Review* (2009) 235-245. I was instructed by the Bar Pro Bono Unit to represent Mr Job, and the presumption was raised in closing speeches, for which see [21], https://journals.sas.ac.uk/deeslr/article/view/1905. James Christie subsequently demonstrated that those responsible in the Law Commission have a great deal to answer for recommending the repeal of section 69 of PACE 1984 and replacing it with the presumption that computers are reliable: James Christie, The Law Commission and section 69 of the Police and Criminal Evidence Act 1984, 20 *Digital Evidence and Electronic Signature Law Review* (2023) 62-69, https://journals.sas.ac.uk/deeslr/article/view/5642.

[6] Michael Jackson, 'An approach to the judicial evaluation of evidence from computers and computer systems' 18 *Digital Evidence and Electronic Signature Law Review* (2021) 50-55, https://journals.sas.ac.uk/deeslr/article/view/5289; James Christie, 'The Post Office Horizon IT scandal and the presumption of the dependability of computer evidence', 17 *Digital Evidence and Electronic Signature Law Review* (2020) 49-70, https://journals.sas.ac.uk/deeslr/article/view/5226; Peter Bernard Ladkin, 'Robustness of software' 17 *Digital Evidence and Electronic Signature Law Review* (2020) 15-24, https://journals.sas.ac.uk/deeslr/article/view/5171.

11. Graham Smith of Bird & Bird LLP raised the point with me that there was little or no case law (that is, mainly appellate in nature) that demonstrates the presumption has been explicitly engaged by a party, although I argue that it was used by the prosecuting Barrister, Warwick Tatford, in the case of Seema Misra.[7] I am grateful to Graham Smith for reminding me of this absence of case law. The scarcity of case law does not mean, of course, that it proves the presumption has never been invoked. The examples of software failure in Chapter 5 of Mason and Seng demonstrates that malfunctions occur, and this is reinforced by newsworthy failure of software that occurs regularly.

The nature of the presumption and its rebuttal

12. It is incontrovertible that the presumption is a rebuttable evidential presumption under common law. This means that to reverse the presumption, all that should be required is for the opponent to cast some doubt as to the reliability of the evidence, or to question if the (mechanical or electronic) system was of a class of reliable devices or was functioning correctly at the material time. To consider this a legal presumption would be to shift the burden of proof to the opponents of such evidence. In criminal proceedings, shifting such a burden onto the defendants undermines the Overriding Objective of the Criminal Procedure Rules, which prioritizes fairness and accurate verdicts. Treating the presumption as a legal presumption would reflect a systemic failure to acknowledge the complexity of digital systems and the risks of uncritical acceptance of electronic evidence.

Rebuttal mechanisms or methods to assist in the authentication of electronic evidence

13. Attempting to rebut such a presumption is demanding. Legal professionals often lack the technical expertise to confront assertions of software reliability, let alone understand how such systems work, while defendants face difficulties securing funding or qualified experts.

14. Even when rebuttal is attempted, judges frequently conflate the presumption with disclosure requirements,[8] rejecting applications for further relevant disclosure on procedural grounds or because of claimed cost.[9] For example, in the Post Office Horizon IT cases, courts failed to recognize that backend system manipulations invalidated the frontend data transaction entries by the subpostmasters and subpostmistresses. This is a technical nuance beyond most judicial understanding for those unfamiliar with client-server architectures and financial processing systems.

15. Effective rebuttal demands specialized knowledge, yet current legal education neglects electronic evidence. As Professor Peter Sommer emphasizes, training for lawyers and judges is essential to bridge this gap.[10] Without such reforms, the presumption remains a de facto barrier to justice.

---

[7] See my analysis of the submissions by the prosecuting Barrister in the trial of Seema Misra in 'The UK Post Office Horizon IT scandal, Part 2: the legal issues', (2024) 30 *Computer and Telecommunications Law Review*, Issue 4, 96-101.

[8] For which see Peter Bernard Ladkin, "Reliable System" in English Law and Reliable Systems (20250130), https://abnormaldistribution.org/index.php/2025/01/22/addressing-the-common-law-presumption-of-computer-reliability-is-a-separate-issue-from-addressing-failure-of-disclosure/.

[9] Regarding the cost of disclosure, see the final exchange between judge Marcus Fabius Quintilian and Sergeant of the Lawe, Sergeant Chaucer in 'Software is reliable and robust' in Mason and Seng, xiii-xiv.

[10] I have been calling for education of the legal profession in a number of editorials of the Digital Evidence and Electronic Signature Law Review: 2007, 2010, 2012, 2016 and 2020. I also commissioned the following articles: Denise H Wong, 'Educating for the future: teaching evidence in the technological age' 10 *Digital*

16. To address these issues, I propose the following framework for the admission and rebuttal of electronic evidence:

    A Code of Practice or Rule of Court, which is regularly updated. Such a Code or Rule could standardize authentication requirements. The *Recommendations for the probity of computer evidence* (2021)[11] outline steps for disclosure and validation, urging courts to adopt these as binding rules.[12]

17. A two-stage authentication process:

    a. Agreement on undisputed evidence: the parties identify uncontested electronic evidence to make proceedings more efficient. These would relate to the typical types of electronic evidence for which the context is such that no substantial disputes as to their authenticity will arise e.g. e-mail exchanges between the parties.[13]

    b. Focused dispute resolution: for contested evidence, courts mandate technical disclosures and expert evaluations.

18. Advisory bodies: establish panels of appropriately qualified and experienced digital evidence professionals to guide rule revisions and advise on emerging technologies.

19. Education: integrate the training of electronic evidence into legal curricula and judicial workshops to improve competency.[14]

20. These mechanisms support the Overriding Objective and promote efficiency while safeguarding against unreliable evidence. The Post Office Horizon IT scandal underscores the urgency of such reforms. Without comprehensive change, miscarriages will persist.

Concluding comments

21. The presumption of computer reliability is incompatible in an era of complex software systems. Authentication must become the foundation of the admissibility of electronic evidence, supported by a Code of Practice or Rule of Court, expert oversight, and legal education. Only through these measures can courts ensure justice in the digital age. This

---

Evidence and Electronic Signature Law Review (2013) 16-24. https://journals.sas.ac.uk/deeslr/article/view/2018; Deveral Capps, 'Fitting a quart into a pint pot: the legal curriculum and meeting the requirements of practice' (2013) 10 *Digital Evidence and Electronic Signature Law Review* (2013) 23-28, https://journals.sas.ac.uk/deeslr/article/view/2019.

[11] Paul Marshall, James Christie, Peter Bernard Ladkin, Bev Littlewood, Stephen Mason, Martin Newby, Jonathan Rogers, Harold Thimbleby, Martyn Thomas CBE, 'Recommendations for the probity of computer evidence', 18 *Digital Evidence and Electronic Signature Law Review* (2021) 18-26, https://journals.sas.ac.uk/deeslr/article/view/5240.

[12] For the complimentary Seven Statement Test, see Alistair Kelman and Richard Sizer, *The Computer in Court A Guide to Computer Evidence for Lawyers and Computing Professionals* (Gower, 1981), updated in Alistair Kelman, *The Computer in Court A Guide to Computer Evidence for Lawyers and Computing Professionals* (e-book, Second edition, 2004), https://docs.google.com/document/d/1cGYi78H0K2pTvQmbdGVroMr7OWFryP5urisy0CYn4nY/edit?tab=t.0.

[13] Contrast *R v Mawji (Rizwan)* [2003] EWCA Crim 3067, [2003] 10 WLUK 438 (discussed in Mason and Seng, 6.123) where other evidence served to corroborate the authenticity of the e-mails in question with *Cole v Carpenter* [2020] EWHC 3155 (Ch), where a claimed e-mail exchange was determined not to be genuine as a result of forensic analysis, https://www.bailii.org/ew/cases/EWHC/Ch/2020/3155.html.

[14] I tried to persuade two English university law departments to work with the digital forensics department (both universities offered a digital forensics course), but neither university pursued the idea.

is particularly pertinent, given the nature of electronic evidence and the rapid moves by software vendors to integrate 'artificial intelligence' into software products.[15]

22. The law cannot be seen to retain this unrealistic presumption. I have given hundreds of seminars to mixed audiences of lawyers and IT specialists across a number of jurisdictions. The consistent response to my explanation of the presumption in English law was a mixture of incredulity, laughter, and disbelief.[16] The development of software and 'artificial intelligence' is accelerating at an astonishing rate. Few industries mandate formal qualifications for software engineers or legally binding technical requirements for the quality of software (certainly not for medical purposes[17]). For this reason, the law must be seen to adopt a more robust and realistic approach to evidence in electronic form than hitherto.

23. We are increasingly required to use and interact with progressively dynamic and connected software systems. I conclude with the observation that it is for the legal profession to take cognisance of the realities of the world in which we now live: to understand the effect of technology on evidence and take realistic and effective action in the interests of justice.

---

[15] For the 3 categories of electronic evidence, see Chapter 3 'Hearsay' and Chapter 4 'Software code as the witness' in Mason and Seng; Daniel Seng and Stephen Mason, 'Artificial Intelligence and Evidence', (2021) 33 *Singapore Academy of Law Journal*, 241-279 https://journalsonline.academypublishing.org.sg/Journals/Singapore-Academy-of-Law-Journal-Special-Issue/Current-Issue/ctl/eFirstSALPDFJournalView/mid/503/ArticleId/1602/Citation/JournalsOnlinePDF.

[16] When speaking in jurisdictions that were not based on Common Law, attendees quickly stopped listening when I spoke about hearsay in the context of electronic evidence. Hence my development of the concept of software as the witness. Discussing the issues in this way always commanded attention.

[17] For an introduction to the issues relating to medical devices, see the work of Harold Thimbleby, Emeritus Professor, Gresham College, London; See Change Digital Health Fellow, Swansea University, Wales; Visiting Professor, UCL, London, in particular his book *Fix IT How to see and solve the problems of digital healthcare* (Oxford University Press, 2021).

Appendix

Questions

We would welcome responses to the following questions set out in this call for evidence.

Questions:

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. See above.

(i) Please specify why you gave this answer

> See above.

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

> Difficult. See the comments that will be submitted by relevant digital evidence specialists.

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

> Education; funding; identifying and then contracting with a suitably qualified professional; knowing what questions to ask; relying on judges to agree to suitable disclosure.

(i) Please give examples where possible.

> See Mason and Seng.

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

> I am not able to comment on this question.

a) As examples of good practice?

b) As examples of things to be aware of?

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:

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

> See the proposal above.

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

> See the proposal above.

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

> See the proposal above.

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?

I am not able to comment on this question.

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

For a definition of 'computer evidence', see the definition in Mason and Seng at 1.113. The three elements are discussed at 1.114. See also the definition in the 'Draft Convention on Electronic Evidence', 13 *Digital Evidence and Electronic Signature Law Review* (2016) S1-S11, https://journals.sas.ac.uk/deeslr/article/view/2321 together with definitions of 'computer', 'electronic evidence', 'electronic record' and 'device'. Note that the 'Commonwealth Draft Model Law on Electronic Evidence and Electronic Evidence: Model Policy Guidelines & Legislative Texts' (Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean, International Telecommunication Union Telecommunication Development Bureau, Geneva, 2013) was drawn upon and referenced in the 'Draft Convention on Electronic Evidence'.

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.

In relation to this issue, the introductory comments are as follows:

We believe that evidence which is merely captured or recorded by a device should be excluded. For example:

Digital communications between people such as text messages, messages sent through web-based messaging services, social media posts, emails;

Digital photographs and video footage;

Breathalyser readouts;

Mobile phone extraction reports.

Superficially, it may appear to be appropriate to exclude some or all of the categories noted in the introductory comments, listed above.

Consider the first example: Digital communications between people such as text messages, messages sent through web- based messaging services, social media posts, e-mails

On the face of it, this might appear to be a simple case of what was written and subsequently extracted.

If the content is only at issue, this fits into Category 1, that is content that is written by one or more people. I agree with the Court of Appeal in that case *R v Mawji (Rizwan)* [2003] EWCA Crim 3067, [2003] 10 WLUK 438

[discussed in Mason and Seng, 6.123]. See footnote 13 above regarding this point.

With all of the examples set out in the introduction to the call for evidence and noted above, the authenticity of the evidence relied upon will depend on the software used by the computer(s) and system(s) that communication, each with the other, to obtain the end result.

It is neither possible nor desirable to think that the items listed by the Ministry of Justice are separated from other software systems.

For instance, a third-party provider (in the case of the Post Office Horizon IT scandal it will have been Fujitsu) might confirm that a computer (without specifying that the computer was part of an integrated system or systems) was working properly and there had been no improper use. Invariably, this assertion will only apply to the process of extracting data from whatever source is it extracted from (e.g. desktop PCs used to compile and dispatch the data). The point being, that the provider will not offer an opinion about the reliability of their computer(s) and/or systems(s) — mainly because they cannot do so — and 'reliability' depends on what is meant by 'reliability' and at what time it (whatever is being considered as 'reliable') was 'reliable'.

An example is given at the beginning and end of the following article:

> Stephen Mason, 'Evidence from computers — the unreliable legal presumption that, without more, it can be relied upon', *The Barrister*, Number 95, 11 January-5 April 2023, 34-35.

The relevant text from the above article is as follows:

Beginning of article:

> *On 16th July I got a fish supper from the Harbour Café, in Girvan, Ayrshire. I paid by @BankofScotland debit card. My statement says I was at the Harbourside Café in Lynmouth, Devon. 450 miles away. It could have been an interesting alibi. "I was in Devon. The bank confirms it." @james_christie, Twitter, 3:21 PM · Aug 22, 2022.*

End of article:

> *The opening quote shows how an alibi supported by apparently reliable electronic evidence could be deceptive. Expert evidence on the quality or otherwise of the electronic evidence would be fraught with difficulties, since virtually the entire electronic system may in fact be working reliably, and an expert could provide evidence that "everything" works. In reality, the error might or*

might not be a problem in the coding interface; or a problem in the café; or the EPOS system; or the bank; or Visa; or Google; or Google's databases; or the cafés' naming or registration with Google; or any other service the bank uses; or any intermediaries, or any combinations thereof. It might be field truncation. It might be errors in cryptographic interfaces. It might be due to an incompatibility with two or more connected systems, neither of which separately has problems. It might even be malicious hacking and nothing to do with the systems as such. It might be human operator error. The point is, everything may appear to be working perfectly, yet the electronic evidence actually has no probative value.

The Ayrshire company has no disclosed links with Lynmouth – the proprietors live in Ayrshire.

The text of the footnote to the end of this sentence reads as follows:

'Scrutinising the contradiction in the claim at the beginning of this article reveals numerous Harbour Cafés up and down the country and none in Lynmouth. The electronic alibi provocatively raised in the opening comment is flawed, as the quote itself suggests. How much other electronic evidence would turn out to be flawed if competently checked? With thanks to James Christie for agreeing to include this example.'

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?

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

About the author

Stephen Mason is a Barrister who is no longer in practice.

Stephen Mason is the joint editor, with Daniel Seng, of the open-source practitioner text *Electronic Evidence and Electronic Signatures* (5th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2021), https://uolpress.co.uk/book/electronic-evidence-and-electronic-signatures/.

Editor of *International Electronic Evidence* (British Institute of International and Comparative Law, 2008) and the author of a number of other legal books.

Founder of the open-source international journal *Digital Evidence and Electronic Signature Law Review* https://journals.sas.ac.uk/deeslr/ which he assigned (together with the annual royalties) in October 2024 to the Institute of Advanced Legal Studies as a gift.

Advised various governments on electronic evidence both directly and on behalf of the Commonwealth Secretariat and took part in similar projects for the European Union and Council of Europe.

Provided professional training for members of the judiciary, lawyers and police officers with the Academy of European Law, American Bar Association, British Computer Society, Council of Europe, European Commission, European Judicial Training Network, International Criminal Court, UNCITRAL, UNESCO and the World Bank amongst others.

Academic external marker in postgraduate degrees dealing with electronic evidence: LLM, University of Oslo (2006); PhD, College of Social Sciences and International Studies, University of Exeter (2013); PhD, Law School, Queensland University of Technology (2015); PhD School of Law, University of Aberdeen (2018).

Visiting Lecturer, School of Law, University of Tartu, Estonia (2017-2021).

Visiting Professor at the Faculty of Law, National University of Singapore (January 2021; September 2025).