

Briefing: Removal of presumption of computer reliability

– Victims and Courts Bill

House of Lords – Committee Stage

4 February 2026

Introduction

1. JUSTICE is a cross-party law reform and human rights organisation working to make the justice system fairer for all since 1957. It is the UK section of the International Commission of Jurists.
2. This briefing calls on peers to support **the new Clause amendment 61 after Clause 12**, in the names of Baroness Chakrabarti, Lord Arbuthnot of Edrom, Lord Beamish and Baroness Kidron.

After Clause 12, insert the following new Clause—

“Removal of presumption of computer reliability

(1) Section 69 of the Police and Criminal Evidence Act 1984 is reinstated.

(2) Section 60 of the Youth Justice and Criminal Evidence Act 1999 is repealed.”

Member’s explanatory statement

This new clause removes the statutory rebuttable presumption that a computer system is working correctly for the purposes of criminal evidence produced by it. Instead, prosecutors would have to offer a reasonable demonstration of the reliability of any relevant hardware and software on which it proposes to rely, thus giving the defence an opportunity to scrutinise and challenge the same.

Background

3. The amendment reinstates section 69 Police and Criminal Evidence Act (“PACE”) 1984 which used to apply in criminal proceedings. It required a party seeking to rely on computer evidence to show:

- (i) there was no improper use of the computer, and
 - (ii) it was operating properly at all material times, or that any faults did not impact the accuracy of the output.
 - (iii) It also allowed for court rules to require further information about the computer evidence.
- 4. After a recommendation from the Law Commission report in 1997,¹ s.69 was repealed in 2000.²
- 5. For the last quarter of a century, a common law presumption has applied instead: that computers producing evidence were operating correctly at the material time. In practice, in the absence of s.69, this means computer evidence is not just *admissible* (i.e. it can be included for consideration) but also is presumed to be *reliable* (i.e. presumed to be accurate) unless that presumption is rebutted.
- 6. This presumption of reliability has led to significant harm most recently in the Post Office Horizon scandal, in which unreliable Horizon accounting software, in which undisclosed errors had occurred, was relied upon in the conviction of sub-postmasters.
- 7. Several Justice ministers have acknowledged the harm since 2018. The Ministry of Justice released a call for evidence over a year ago, on 21 January 2025, on the “Use of evidence generated by software in criminal proceedings.”³ It is yet to release any policy or government response.

What is the problem?

- 8. The current presumption is **inaccurate**, **unsafe**, and **not future-proof**.

Inaccurate

- 9. **Technology is buggy:** The presumption that computers are working reliably is a legal fiction. We know that computers are fallible and there has been growing concerns for years about the current law. For example, in 2006 Van Buskirk and Liu observed: “*There is a general tendency among courts to presume – without the benefit of meaningful assurance – that forensic software*

¹ Law Commission, ‘[Evidence in Criminal Proceedings: Hearsay and Related Topics](#)’, Report no. 245, 1997

² By Section 60 of the Youth Justice and Criminal Evidence Act 1999

³ Ministry of Justice, [Call for Evidence: Use of evidence generated by software in criminal proceedings](#) (21 January 2025)

can be trusted to yield accurate digital evidence. As a judicial construct, this presumption is unjustified in that it is not tailored to separate accurate results from inaccurate ones.”⁴

10. **Errors can be latent, not blatant:** Even safety critical computer systems contain errors in their code which many not be evident at first glance.^{5 6} The presumption therefore does not match the reality of computer systems: they cannot be assumed to be reliable, even when they appear to be working.
11. **Wide commercial recognition of software errors as commonplace:** As raised by Baroness Kidron during the Data Use and Access Act debates, software contracts for the last 20 years have included disclaimers such as “No warranty is provided that the operation of the software will be uninterrupted or error free, or that all software errors will be corrected.”⁷ As she concluded “it is a presumption that anyone with even the most basic knowledge of computers would consider absurd.”

Unsafe

12. The presumption is rebuttable. It could *in theory* operate safely if it were easy to rebut when there is a reasonable concern about the reliability of the computer evidence and processes in place to ensure fair challenge. However, there are several reasons this does not happen in practice.
 - (a) **Knowledge imbalance:** In an adversarial system, a defendant stands little chance of rebutting the presumption if they have no knowledge of an error. In the Post Office Horizon cases, the software error involved a bug – which was “*impossible for users to*

⁴ Eric Van Buskirk and Vincent T. Liu, ‘Digital evidence: challenging the presumption of reliability’ (2006) (1) *Journal of Digital Forensic Practice* 19, 20, original emphasis.

⁵ Peter Bernard Ladkin, Bev Littlewood, Harold Thimbleby and Martyn Thomas CBE, ‘[The Law Commission presumption concerning the dependability of computer evidence](#)’, 17 (2020) *Digital Evidence and Electronic Signature Law Review*, 6: “There is a general consensus in some areas of the safety critical systems community that a fault density of about 1 per kLoC [“kLoC” is one thousand (kilo) lines of code] is world class. Some software ... is rather better but fault densities of lower than 0.1 per kLoC are exceptional. The UK [Ministry of Defence] funded the retrospective static analysis of the [Hercules] C130J [transport aircraft] software, previously developed to [civilian aerospace software standard RTCA] DO-178B, and determined that it contained about 1.4 safety-critical faults per kLoC (the overall flaw density was around 23 per kLoC...whilst a fault density of 1 per kLoC may seem high it is worth noting that commercial software is around 30 faults per kLoC, with initial fault injection rates of over 100 per kLoC”.

⁶ See further James Christie, ‘The Law Commission and section 69 of the Police and Criminal Evidence Act 1984’ *Digital Evidence and Electronic Signature Law Review*, Vol 20 (2023) 67.

⁷ House of Lords, *Data Use and Access Bill [HL]* Committee Stage, Volume 842, Wednesday 18 December 2024, [Column 154GC](#)

detect.⁸ The error logs were disclosed for the first time in 2018⁹ during the High Court litigation, years after the last of the criminal prosecutions, and were of “*central importance to [Fraser J’s] judgment*” that the technology caused shortfalls in the accounts and the Horizon computer evidence was unreliable.¹⁰

- (b) **Inequality of arms:** This imbalance of knowledge was exacerbated in the Post Office prosecutions by inequality of arms. Tracy Felstead’s¹¹ barrister, Paul Marshall, has explained the financial barrier imposed in her case to rebut the presumption:

‘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.’¹²

- (c) **Lack of transparency of private actors:** the fact that the known error logs were in the possession of a private actor, Fujitsu, and not the Post Office, also suggests that a further barrier is lack of transparency and inaccessibility in procurement arrangements, through expense or for other reasons, of critical information relating to the reliability of the computer system’s functioning when prosecutors are relying on computer systems maintained or supplied by the private sector.
- (d) **Cultures of over-trust in IT:** It is a wider issue than the Post Office Horizon scandal. Professor Harold Thimbleby,¹³ expert witness in computer science for criminal proceedings involving the prosecution of nurses for wilful neglect based on corrupted

⁸ Christie (2023)

⁹ 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 and Electronic Signature Law Review (2021) 18, p.19.

¹⁰ *Bates v Post Office Ltd Rev 1 (Horizon Issues)* [2019] EWHC 3408 (QB) at [18].

¹¹ Tracy Felstead was one of 39 sub postmasters cleared by the Court of Appeal.

¹² Paul Marshall, [‘Failed Justice –how commercial interests displaced the interests of justice in the Post Office Case’](#), Queen’s University Belfast, Institute of Professional Legal Studies, 2022.

¹³ Professor Emeritus of Computer Science, Swansea University

hospital data, has recounted widespread misunderstandings of IT and data in the hospital system, police and legal systems, leading to a poor IT culture which accepts computer evidence at face value.¹⁴

- (e) **Rights-impact: reversal of the burden of proof:** If no proof is required that computers are properly functioning, as currently is the case, then the prosecution is benefitting from a shortcut to proving its case. When the burden of rebutting the presumption is too onerous, for reasons of lack of knowledge, inequality of arms, or inaccessibility of information held by private third parties, then in effect there has been a reversal of the burden of proof. Defendants are struggling to prove their innocence, rather than prosecutors proving their guilt. This undermines a key tenet of a fair trial: the presumption of innocence.

Not future-proof

- 13. The law was changed and s.69 PACE repealed at the recommendation of the Law Commission in 1997. This was before Google, the iMac, Youtube, Twitter, Facebook, the iPhone, let alone the current AI “boom” enabled by complex machine and deep learning. A lot has changed, and JUSTICE considers the presumption to be even less safe looking to the future.

- (a) **AI:** Emerging technologies under the umbrella term of artificial intelligence (“AI”)¹⁵ are being integrated into all areas of society. A lot of the computer systems referred to as AI generate outputs not through simply “deterministic” or rules-based processes, but also through probabilistic processes and sometimes stochastic, i.e. random, processes. Critically, what computers are doing is becoming increasingly complex, and there can be technical and commercial reasons for barriers to transparency, explainability and interpretability.¹⁶ Simply assuming “proper working” for such computer evidence will be inaccurate and unsafe.
- (b) **Deepfakes:** Generative AI can produce extremely convincing but wholly erroneous or misleading information, in the form of text, audio and/or visual outputs. Sometimes

¹⁴ Harold Thimbleby, ‘Misunderstanding IT: Hospital cybersecurity and IT problems reach the courts’ (2018) *Digital Evidence and Electronic Signature Law Review* 15, 11-32.

¹⁵ JUSTICE adopts the OECD definition of AI, updated in May 2024, as follows: “An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.” See OECD, [Explanatory memorandum on the updated OECD definition of an AI system](#) (2023).

¹⁶ See JUSTICE, [AI in our Justice System](#) (2025)

known as deepfakes, when created intentionally, such technology is available to anyone with an internet connection, often at no cost, as has been seen recently with the use of Grok AI to create non-consensual digitally altered images of women and children without their clothes on.¹⁷ This technology therefore signals a shift in the scale of the threat of mis- and disinformation, including in justice systems. Our courts need to be armed with evidence law which enables them to deal with such computer outputs critically, rather than through unsafe and inaccurate presumptions.

What is the solution?

14. JUSTICE considers the legal presumption is no longer fit for purpose. Reinstating s.69 would:
 - (a) **Better reflect reality:** that computers are fallible, software is buggy, and the presumption is unsafe.
 - (b) **Put the burden of assurance back on those relying on the evidence:** it necessitates a party makes some inquiry about whether the computer was working at the material time, which the current law dissuades.
 - (c) **Prevent miscarriages of justice:** by stopping unsafe computer evidence, which cannot be shown to have been working properly, or not tampered with, coming into court proceedings.
 - (d) **Enable courts to better control the evidence:** S.69(2) allows the courts to make rules and demand further information, which will help courts respond to advancing technology by creating rules for better disclosure of information relevant to computer evidence reliability, e.g. error logs, certification, and audit trails.
15. JUSTICE urges Peers to support the amendment, and question the Government on the delay in responding to its own call for evidence on the topic, which was released over a year ago.

For more information, please contact:

Ellen Lefley, Senior Lawyer, JUSTICE – elefley@justice.org.uk

¹⁷ See for example, Laura Cress, [Woman felt 'dehumanised' after Musk's Grok AI used to digitally remove her clothes](#), BBC News (2 January 2026)