# Avoiding Future PO Horizon-like Miscarriages of Justice - the Expert Way

*by Dr Stephen Castell CITP MEWI*

*Dr Stephen Castell is an award-winning software and systems consultant professional, IT and the Law pioneer, and FinTech visionary, active as an international expert witness in major complex computer systems and technology development disputes and litigation, including the largest and longest such actions to have reached the English High Court, and appointed in the ongoing high-profile FTX, Voyager and Binance US Class Action cryptocurrency lawsuits.*

**Introduction**

It took an ITV broadcast dramatization, Mr Bates vs. the Post Office, for the PO Horizon affair to gain enough public outrage to get the attention of the UK government to do something, fast, to rectify the damage caused to many hundreds of PO Sub-Postmasters and Postmistresses, and their families, arising from private prosecutions brought by the Post Office, sustained over twenty years, 1999-2019, prosecutions that wrongfully relied on the evidence of the faulty Horizon computer system – described as the 'greatest ever miscarriage of British justice'.

The trials of those falsely accused by the Post Office were conducted on the legal presumption that computer-generated evidence should be treated as completely trustworthy, unless the defence could explicitly prove that it was faulty. This was the crucial, but wrong-headed, forensic foundation of the whole sorry 20-year PO Horizon travesty of justice.

But how did this happen? My 1980s VERDICT & APPEAL studies for HM Treasury, bringing in the **admissibility** of computer evidence in court (PACE 1984), was later mangled by the Law Commission into its 1999 'legal presumption of the **reliability** of computer evidence', without which the PO would never have so easily bamboozled the courts into ignoring the Horizon system bugs. That 'presumption', and, equally, the lack of Legal Aid funding to enable Defendants to engage expert witnesses on their behalf, to insist on disclosure of, and thus be able to challenge and rebut, the Horizon evidence against them, is at the very heart and foundation of the whole tragic Horizon affair. (Back in 1999-2000, I myself was approached to be expert witness on behalf of one of the first Sub-Postmistress Defendants, but Legal Aid funding to appoint me could not be obtained. Had I actually been engaged, with adequate budget for investigation, I am pretty sure that I would have discovered the Horizon bugs, and revealed that a prosecution based on such a faulty system would clearly

have been unsafe – and perhaps then the whole sorry twenty-year saga could have been avoided).

As importantly, in my VERDICT & APPEAL studies for HM Treasury, which, following my recommendations, brought in the admissibility of computer evidence in court (before that it risked being treated only as 'hearsay' evidence), I had also made clear that "A trial that seeks to **rely** on computer evidence must first be a trial **of** that computer evidence" but this equally significant rider was later ignored by the Law Commission. The Horizon tragedy now graphically reveals the truth of my recommendation, and corrective change is now well overdue – the infamous wrongheaded 'presumption of reliability' must go, and now. We have a group of IT savvy experts and lawyers who do not intend to stop until we get that erroneous 'legal presumption of the reliability of computer evidence' repealed.

Meanwhile, everyone needs to be aware that there is the real and present danger of 'future Horizons' out there. More Horizon-like fiascos could for sure be brewing, since complex IT systems always have bugs and the whole economy, and government, has become more and more reliant on such interconnected systems, on an unquestioning 'computer says no' basis. This article briefly sets out the Professional ICT Expert way to try to identify and avoid such 'future Horizons', based on established principles of resolutely seeking and obtaining full disclosure of all computer evidence relevant to the case, plus expert challenges to the forensically unsound reliance on a 'computer evidence is always trustworthy' presumption.

**Avoiding 'Future Horizon' IT Disasters**

From an experienced expert witness perspective, the profiles of many, if not all, IT software and systems project and implementation disasters exhibit almost exactly the same sort of issues as featured in the PO Horizon matter. As set out in my 2006 Cutter Consortium Executive Report, the critical issue is whether or not there are software material defects in the systems(s) on whose evidence the case relies: it is therefore vital for independent expert witnesses to have disclosed all relevant system details, and the associated digital evidence to be adduced, so that appropriate specialist examination and rebuttal of such computer evidence may be pursued in good order.

So the principal forensic process is quite simple: as noted earlier, 'A trial that seeks to **rely** on computer evidence must first be a trial **of** that computer evidence'. This disclosure and probing of the computer evidence happens routinely in Civil actions, where the parties privately pay experts on both sides to examine carefully all digital evidence disclosed, and the skilled forensic IT professionals appointed as expert witnesses diligently assess whether or not there are indeed software material defects.

However, in Criminal prosecutions, there is very often a denial of sufficient access to and employment of independent expert witnesses on behalf of the Defendant, since the UK Legal Aid system is simply not funded adequately and therefore not ft for purpose in regard to this vital IT expert resource, essential for the proper and fair administration and delivery of justice.

Whether there may arise the possibility of a Civil action, or a Criminal prosecution, involving and relying on computer evidence, for your company, organisation, government department, firm, association, or other institution it would be advisable and sensible to try to avoid any Horizon-like disaster coming to your door or brewing unnoticed within.

So, here are three essential steps for companies, organisations, and their lawyers, designed and targeted to provide that timely avoidance:

**Step 1.** Engage asap an experienced independent skilled and experienced forensic ICT expert professional to carry out a **Litigation-Sensitivity Audit** of your planned or ongoing mission-critical public-facing IT systems projects. Ideally, this should be at the initial conception or ideas stage, but the earlier into any such anticipated or actual software and systems project lifecycle this is done, the better.

**Step 2.** Scope, Resource and Empower this engagement to allow the independent forensic ICT expert professional to:

• Have full access to your software, systems, project management documentation, records, logs, data, results and people involved. This should include both internal staff and that of any contractors, at all levels.

• Examine in detail your full software development project details: the requirements specification, design documentation, coding development records and workings, and systems testing data, results and logs.

• Assess the research and records of any marketing feedback, 'satisfaction survey data', complaints, Help Desk Ticket logs etc available from the users (or anticipated users) of your company's existing and planned systems.

• Report direct (and interactively) to your C-level executive team the findings, conclusions and recommendations of the Litigation-Sensitivity Audit.

**Step 3.** Commit to and Resource a Meaningful and Effective Board Level Response to the presentation of the analyses, findings and recommendations given in the Litigation-Sensitivity Audit produced by the independent forensic ICT expert professional to:

• Identify and scale the risks and likelihoods of serious consequences to employees, users and the public at large in or arising from the definition, design, construction, testing, user-training, deployment, operation and governance of your planned or ongoing mission-critical public-facing IT systems projects.

• Put in place effective monitoring of those systems to allow you to have timely oversight and trouble-shooting of any such potential serious consequences, before they escalate.

**Conclusion**

Following these three steps, involving engagement of an experienced independent skilled and experienced forensic ICT expert professional to carry out a Litigation-Sensitivity Audit, should provide a workable dynamic framework to be able to identify, and avoid, your planned or ongoing mission-critical public-facing IT systems projects developing into potential 'Future Horizon' IT Disasters. If these steps are not followed, there is a chance that you may move suddenly to the 'Disaster Step', where perhaps a television dramatization, similar to Mr Bates vs. the Post Office, this time reveals that it is your company that, for years, has been culpably operating computer systems causing serious life-changing financial and other consequences to employees, users and/or the public at large. And however that revelation may pan out, you can 'reliably presume' that the experience will not be a pleasant one.

**Background Reading**


BCS IT Leaders Forum, 2023. 'SERVICE RESILIENCE AND SOFTWARE RISK', NOVEMBER 2023, 16 pages: "The UK Government Resilience Framework1 is built around three fundamental principles:

• That we need a shared understanding of the risks we face;

• That we must focus on prevention and preparation; and

• That resilience requires a whole of society approach. This report identifies the risk from software failure as a hurdle to national resilience; resilience is defined as "action to prevent or mitigate risk". We – people and organisations in the UK – are increasingly dependent on services that are at risk from software failure. This report makes recommendations to prevent software (defined as "the programs and other operating information used by a computer") failures and to mitigate the risk from these software failures to the resilience of service delivery…".

Castell, S., 2023. "Computer Evidence: presume nothing, trust no software or data, engage an expert. Costly? Just look at the cost if you don't. Challenging the reliability of AI and other complex multi-connected intelligent computer systems will become of fundamental importance as businesses and society move rapidly towards a software-dominated, algorithm-governed future. Increasingly ubiquitous 'algo dependency' is likely to result in a wide variety of disputes, some of which will reach court, in which computer evidence will critically feature. …", by Dr Stephen Castell CITP CPhys FIMA MEWI MIoD, Barrister Magazine, January 19, 2023.

Castell, S., 2022. "New Financial Risks Arising from Digital Finance: Disputes Over Automated Decision Systems and Algorithmic Assessments by ICT Forensic Expert Witnesses", Acta Scientific Computer Sciences, Volume 4 Issue 7 – 2022 (Published July 01, 2022): 24-36.

Castell, S., 2021. "A trial relying on computer evidence should start with a trial of the computer evidence. Learning from the Post Office Horizon scandal …", Computer Weekly, 22 December 2021.

Castell, S., 2021. "Direct Government by Algorithm Towards Establishing and Maintaining Trust when Artificial Intelligence Makes the Law: a New Algorithmic Trust Compact with the People", Acta Scientific Computer Sciences 3.12 (2021): 04-21, November 10, 2021.

Castell, S., 2021. "Block Chains and Stablecoins", ExpertWitness.co.uk, January 7, 2021.

Castell, S., 2021. "Blockchain and Cryptocurrency Tracing Disputes: Digital Forensics Evidential Standards", Experts.com, articles.

Castell, S., 2006. "Forensic Systems Analysis: A Methodology for Assessment and Avoidance of IT Disasters and Disputes", issued as a Cutter Consortium Executive Report, Enterprise Risk Management & Governance Advisory Service series, Vol. 3, No. 2, 8 March 2006.

Castell, S., 2003. "Role of the IT expert witness: The role of the IT expert witness in software and systems development/implementation contract disputes and litigation", Computer Law & Security Review, 19(3):228–231, May 2003.

Castell, S., 1996. "Seeking after the truth in computer evidence: any proof of ATM fraud?", The Computer Bulletin, Volume 38, Issue 6, December 1996, Pages 17–19.

Castell, S., 1994. "A computer of the simplest kind", Computer Law and Security Report, 10, May-June 1994 (and see further references under its 'FOOTNOTES'). Cited in Mason, S., and Townley, L., "Competence of witnesses", Chapter 10, para 10.15, 'Electronic Evidence and Electronic Signatures', 2021, University of London Press, Pages: 60.

Castell, S., 1993. "Computers trusted, and found wanting", Computer Law and Security Report, 9, July-August 1993, pp. 155-156.

Castell, S., 1991. "Computers out of control", Financial Times, May 29, 1991, Wednesday, SECTION I; Letters, Page 19.

Castell, S., 1990, The APPEAL Report, May, Eclipse Publications, ISBN 1-870771-03-6.

Christie, J., 2023. "Law Commission misrepresented experts when it changed rule on computer evidence. The Law Commission repeatedly quoted vague, arm-waving, un-evidenced comments by judges who offered no insight into anything beyond their own technical ignorance. The law change made miscarriages of justice inevitable. …", Computer Weekly, 02 Nov 2023.

Flinders, K., 2024. "More than 900 subpostmaster convictions wouldn't have happened without Post Office-backed law change. IT expert says it cannot be the case that computer evidence is treated as accurate in court, without investigation into surrounding circumstances…", by Karl Flinders, Chief reporter and senior editor EMEA, Computer Weekly, 18 Jan 2024.

Flinders, K, 2022. "Government has no plans to review controversial court rules on computer evidence. Government accused of 'passing the buck' and

'not knowing what it is talking about' …", Computer Weekly, 23 May 2022.

Fry, J., 2023. "Has the Law Commission got it wrong regarding a 'new, third type of property asset'?", Written by Dr. Stephen Castell, Published in Coinmonks, Aug 16, 2023.

Hyde, J., 2021. "News focus: Post Office Horizon scandal – Where weren't the lawyers? There are calls for a full, judge-led public inquiry into the Post Office prosecution of former subpostmasters, with many wondering what role lawyers played in this miscarriage of justice…", The Law Society Gazette, 3 May 2021.

Meddings, S., 2022. "Should those who sent the subpostmasters to prison now face court themselves? Sub-postmasters were hounded for years, even after doubts were raised over the IT evidence that convicted them. Despite this, their prosecutors remain unrepentant", The Times, Saturday August 06 2022.



**Dr Stephen Castell**
CITP CPhys FIMA MEWI MIoD
Chairman, CASTELL Consulting
PO Box 334, Witham, Essex CM8 3LP, UK
Tel: +44 1621 891 776
Mob: +44 7831 349 162
PO Box 270529, San Diego, CA 92198, USA
Tel: +1 310-890-9859
Email: stephen@castellconsulting.com
http://www.e-expertwitness.co.uk
https://archivesit.org.uk/interviews/stephen-castell/
January 21, 2024