Ensuring Computer Reliability After The Post Office Horizon Scandal



As the enquiry into the Post Office Horizon scandal continues, Harold Thimbleby explores this and other cases where IT system failures have had significant impact on welfare and safety. He discusses the legal factors that make it hard for IT systems to be called into question, and proposes measures that could be taken to prevent these issues arising again in the future.

In the UK, the Post Office prosecuted nearly 1,000 postmasters — plus more who settled out of court — for fraud, theft, and false accounting. The evidence used in court is now known to have been corrupted by bugs and unauthorised access to the Post Office's Horizon computer system. The Court of Appeal Judge said the Post Office's malicious prosecutions and failures were so egregious as to make the prosecutions an affront to the conscience of the court. Following the powerful 2024 ITV drama *Mr. Bates vs The Post Office* about the problem the Government promised to cancel prosecutions and pay compensation, and has since passed the Post Office (Horizon System) Offences Act 2024, which has exonerated and ordered compensation for many (but not all) affected postmasters.

Horrendous as the Post Office IT case has turned out to be, it's by no means unique.

In the Netherlands the prime minister, Mark Rutte, and his Government resigned in January 2021 after more than 1,000 children had been forcibly taken into care because SyRI, a computer system used for predicting fraud, had erroneously charged people with fraud and demanded payments of hundreds of thousands of euro. A Dutch court ordered the government to stop using SyRI as it violated human rights and had ruined thousands of lives.

In Australia, a computer system called Robodebt led to welfare recipients having to pay non-existent debts. The burden of proof was moved from the system needing to verify the information to the individuals having to prove they didn't owe anything. In 2022, the Australian government finally forgave the debts of 197,000 people.



In 2024, CloudStrike's routine cybersecurity update crashed 8.5 million PCs worldwide, including putting many healthcare systems from Australia to the UK out of action. Delta Airlines who suffered major problems was served a class action suit by passengers, and in turn Delta blamed CrowdStrike for its $500m loss — yet Delta would have signed off CrowdStrike's software disclaimer, which says *"TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW CROWDSTRIKE SHALL NOT BE LIABLE."*

That such ubiquitous end user licence agreements (EULAs) have force is underlined by Disney who argued in court that, as a person who died from an allergic reaction to food served in a Disney Park had agreed to a EULA for a free trial of a Disney streaming service, that therefore the court should compel arbitration and stay the proceedings against them. The Disney EULA states *"You and Disney DTC agree to arbitrate, as provided below, all disputes between you (including any related disputes involving The Walt Disney Company or its affiliates)"* However a major public backlash against Disney led them to "waive their right to arbitration" which simultaneously makes them look good yet retains the sweeping interpretation of the EULA.

The NHS as a whole is riddled with IT problems too, as is made clear by the booklet: *Patient Safety — Stories for a digital world*, available at https://www.harold.thimbleby.net/booklet





The Royal College of Anaesthetists advise doctors that they should ignore the output of any computer monitoring, and make all necessary clinical observations and controls themselves. The reason is that the technical specification of the equipment and the programs are "commercial in confidence" and therefore cannot be trusted because nobody who knows (if anyone does!) will tell the anaesthetists exactly how they work.

Like the Post Office case, many NHS IT problems surface in court with unfortunate results, often prosecuting nurses for problems caused by inadequate computer systems.

James Christie shows that lawyers and the law itself do not understand IT [1]. Central to the Post Office's approach to prosecution was the flawed common law presumption that computer evidence is correct [2]. In practice, this evidential presumption turns "innocent until proven guilty" on its head, reversing the burden of proof on the defendant to show why the computer evidence should not be relied on as a true statement of fact. This is nearly impossible to do as the presumption cannot easily be rebutted. In many cases, the legal presumption undermines justice, but it also insulates the courts from technical arguments that would go over everyone's heads. Justice isn't served either way.

Artificial Intelligence is making the problems more acute. Generally, nobody really understands how AI works, as it isn't just programmed by humans (with enormous programs that themselves will contain bugs) but also learns, and can learn anything from incorrect and misleading data. Indeed, bias (such as gender and racial bias) in data is recognised as a serious problem. Worse, AI companies make amazing promises so AI has become irresistible to adopt in all sorts of areas, and adoption is happening much faster than we understand how to use it safely. Police profiling, driverless cars, credit rating systems, and medical diagnosis are just some of the areas where AI has already created problems after removing human oversight.

Regulating AI has become an internationally-recognised concern, but strangely there has been little interest in regulating IT more widely, let alone regulating professional developers. Regulation in other critical areas is broader; for instance in mains electricity, not just the products are regulated, but the types of use and the electricians themselves are regulated too. Moreover, in electrical and other safety critical industries there are rarely complaints about regulatory burden or stifling innovation through regulation.



VICTORIÆ REGINÆ.

CAP. XC.

In the nineteenth century, Parliament passed the Medical Act of 1858 in response to the scandal that people were being treated by dangerous quacks instead of by competent doctors. In the Act's opening words, *"it is expedient that Persons requiring Medical Aid should be enabled to distinguish qualified from unqualified Practitioners."*

Why not adopt this attitude in IT? Indeed, many doctors' treatments are delivered by IT (for instance, with drug delivery systems like computerised infusion pumps) and surely those NHS computers should be as at least reliable as doctors are required to be? Yet they aren't [3].

One can anticipate that there will be opposition to any apparent increase in regulatory burden for assuring reliable IT systems — there are many large companies and people involved in the industry who would lose work and whose products would lose value or become unsellable. While the problems of failures of cowboy IT systems are not going to be completely solved [4], surely they can and should be controlled a bit better before more catastrophes happen?

There is obviously scope for a lot of debate about how to improve the reliability of computers. Here are some starter ideas:

- Our first proposal thing would be to fix EULAs. Ban use of evasive terms such as "professional intermediary" (terms which try to make the user liable), and EULAs that explicitly require users to indemnify manufacturers. Once we start considering improvements, there are many ways to improve EULAs, for instance why not void blanket terms that are frequently abused, such as in the Disney case above.
- Next, the Health and Safety At Work (HSAW) Act should be brought up to date with IT. The Act currently says every employer must ensure, so far as is reasonably practicable, that both employees and persons not in their employment are not exposed to risks to health or safety, including undertaking research and testing to minimize such risks — but nobody properly enforces the Act's stipulations across IT yet.
- If EULAs were tightened and the HSAW brought up to date with IT, manufacturers would soon start employing more competent programmers, and then the Medicine Act analogy would seem less far-fetched.
- This list isn't intended to be complete in any way, for instance it doesn't explore any technical opportunities, such as digital certificates, etc.

What are your ideas? Do email harold@thimbleby.net

With acknowledgements to the whole team who authored [2] and helped improve this article.

Further reading

[1] J Christie, "The Post Office Horizon IT scandal and the presumption of the dependability of computer evidence," *Digital Evidence and Electronic Signature Law Review*, **17**:49–70, 2020. DOI 10.14296/deeslr.v17i0.5226

[2] N Bohm, J Christie, PB Ladkin, B Littlewood, P Marshall, S Mason, M Newby, SJ Murdoch & M Thomas, "Briefing Note: The legal rule that computers are presumed to be operating correctly — unforeseen and unjust consequences," *Digital Evidence and Electronic Signature Law Review*, **19**:123–127, 2022. DOI 10.14296/deeslr.v19i0.5476

[3] H Thimbleby, *Fix IT — See and solve the problems of digital healthcare*, Oxford University Press, 2021. See also https://www.harold.thimbleby.net/booklet

[4] H Thimbleby, "Cowboy digital undermines safety-critical systems," *Safer Systems: The Next 30 Years, Proceedings of the 30th Safety-Critical Systems Symposium*, ed M Parsons & M Nicholson, **SCSC-161**:203–226, Safety-Critical Systems Club, 2022.

Image attribution:
front: Wellcome Library, London, CC BY 4.0, via Wikimedia Commons
crowdstrike ID 327905900 © Valeriia Lukashova | Dreamstime.com
diagnostics: OpenStax, CC BY 4.0, via Wikimedia Commons
Medical act | Legislation.gov.uk licensed under Open Government Licence v3.0

Harold Thimbleby

Prof Harold Thimbleby is See Change Fellow in Digital Health at Swansea University, Wales. Harold won the BCS Wilkes Medal and has previously been a Royal Society Wolfson Research Merit Award Holder. He has published over 300 refereed papers, and has given over 600 presentations around the world.

The author retains copyright of this article.