The legal rule that computers are presumed to be operating correctly – unforeseen and unjust consequences

Overview

1. In England and Wales, courts consider computers, *as a matter of law*, to have been working correctly unless there is evidence to the contrary. Therefore, evidence produced by computers is treated as reliable unless other evidence suggests otherwise. This way of handling evidence is known as a 'rebuttable presumption'. A court will treat a computer as if it is working perfectly unless someone can show why that is not the case.

2. This presumption poses a challenge to those who dispute evidence produced by a computer system. Frequently the challenge is insurmountable, particularly where a substantial institution operates the system.

3. The Post Office Horizon scandal clearly exposes the problem and the harm that may result. From 1999, the Post Office prosecuted hundreds of postmasters and Post Office employees for theft and fraud based on evidence produced by the Horizon computer system showing shortfalls in their branch accounts. In those prosecutions, the Post Office relied on the presumption that computers were operating correctly.

4. Hundreds of postmasters and others were convicted, sentenced to terms of imprisonment, fined, or had their property confiscated. This clearly demonstrated that the Law Commission's assertion that 'such a regime would work fairly' was flawed.

5. In the December 2019 judgment in the group litigation *Bates v The Post Office Ltd (No 6: Horizon Issues) Rev 1*,[1] Mr Justice Fraser concluded that it was possible that software errors in Horizon could have caused apparent shortfalls in branch accounts, rather than these being due to theft or fraud.[2] Following this judgement, the Criminal Cases Review Commission referred an unprecedented number of convictions, based upon the supposed shortfalls in the Horizon accounts, to the Court of Appeal. Appeal courts have quashed more than 70 convictions at the time of writing. There will be many more appeals and many more convictions quashed in what is likely the largest miscarriage of justice in British history.

6. Were it not for the group litigation, the fundamental unreliability of the software in the Post Office's Horizon computer system would not have been revealed, as previous challenges to Horizon's correctness were unable to rebut the presumption of reliability for computer evidence. The financial risk of bringing legal action deterred other challenges. Similar issues apply in other situations where the reliability of computer evidence is questioned, such as in payment disputes.

7. The legal presumption, as applied in practice, has exposed widespread misunderstanding about the nature of computer failures – in particular, the fact that these are almost invariably failures of software. The presumption has been the cause of widespread injustice.

8. There is a pressing requirement for the presumption to be re-evaluated to avoid the risk of further or continuing injustice.

9. We propose that the presumption that computer evidence is reliable be replaced with a process where if computer evidence is challenged, a party must justify the correctness of the evidence upon which they rely. The proposed process, summarised below, requires the disclosure of documents that would already exist in any well-managed computer system. The procedural and evidential safeguards of the kind we propose would probably have avoided the disastrous repeated miscarriages of justice over the past 20 years.

Background

The legal position from 1984

Once computers began to be used in everyday life, it was necessary to consider how evidence

in electronic form was to be presented in legal proceedings. A document produced by a computer is 'hearsay' evidence, the kind of evidence that the courts treat with caution because a person relying upon it has no direct personal knowledge. While such evidence was admissible, courts needed to decide how reliable it was and what weight could be placed upon it.

A solution was provided by section 69 of the Police and Criminal Evidence Act 1984 (PACE 1984), that required the prosecution to prove that a computer was operating properly at the relevant time before a document produced by such a computer could be admitted as evidence. As the volumes of computer evidence increased, this requirement became burdensome and inconvenient.

The Law Commission: the proposed change in the law

In 1997, the Law Commission published a paper *Evidence in Criminal Proceedings: Hearsay and Related Topics*.[3] Computer evidence was considered in Part XIII. Reviewing the problems faced by prosecutors, the Law Commission considered the law to be unsatisfactory and expressed its view that PACE 1984 s69 served 'no useful purpose.'[4] It proposed that s69 should be repealed (and not replaced) with the effect that:[5]

> 'In the absence of evidence to the contrary, the courts will presume that mechanical instruments were in order at the material time.'

The Law Commission considered that the words 'mechanical instruments' would extend (by default) to include computers.[6]

The law is changed

Section 69 of PACE 1984 was repealed by the Youth Justice and Criminal Evidence Act 1999. The result was that the law makes the presumption that the Law Commission identified and recommended.

The purpose of a presumption

The aims of a presumption, that allocates the burden of proof between the parties to legal proceedings, are to:

1) alleviate the need to prove every item of evidence,

2) reduce the need for evidence in relation to some issues, and

3) to save 'the time and expense of proving the obvious.'[7]

The reason for changing the law

In principle, there is a low threshold for rebutting the presumption that computer evidence is reliable. If such a challenge succeeds, the *burden of proof* lies with the party relying upon such a document to prove it, thus proving its source's integrity and reliability. In a criminal trial, that burden is to the criminal standard.

The Law Commission admitted that there was a practical problem in challenging the evidence:[8]

> 'The question is, what sort of evidence must the defence adduce, and how realistic is it to suppose that the defence will be able to adduce it without any knowledge of the working of the machine? ... It could therefore take very little for the presumption to be rebutted, if the party against whom the evidence was adduced could not be expected to produce more.'

The Law Commission also said:[9]

> '... that the burden would be interpreted in such a way as to ensure that the presumption did not result in a conviction merely because the defence had failed to adduce evidence of malfunction which it was in no position to adduce. We believe, as did the vast majority of our respondents, that such a regime would work fairly.'

The presumption is unsafe

The presumption is unsafe because the belief that it would work fairly has been shown to be unjustified and wrong. That it is unsafe is put beyond sensible dispute by the findings of Mr Justice Fraser in his 2019 judgment.[10] The judgment shows that errors in computer systems, specifically software defects (bugs), *may not be readily apparent* and, on the contrary, be difficult to identify. Bugs may cause a computer system to

work very differently from the intended behaviour, with unexpected – sometimes devastating – consequences. The effects of such bugs in the Post Office Horizon computer system were not readily observable or identifiable to postmasters and others prosecuted by the Post Office.

Consequently, those prosecuted had no means by which to effectively (or at all) challenge the reliability or integrity of the Horizon computer system. They had no means of providing to the court *evidence capable of rebutting the presumption*. Rebutting the legal presumption may, in practice, present insuperable problems for defendants, and in the Post Office prosecutions did so.[11]

The presumption fails to make the crucial distinction between computer hardware and software. In fact, the great majority of failures of computer systems are attributable to failures of software – as indeed was the case for the Post Office Horizon system.

How the presumption has worked in practice

The way in which the legal profession has dealt with 'the presumption' has led to significant unfairness and injustice, as revealed by the wrongful conviction of postmasters and others in the Post Office Horizon prosecutions from the turn of the century. It is unknown how many other prosecutions will have been affected by the presumption.

While the convenience that was sought through repealing s69 of PACE 1984 is understandable, a presumption that a computer 'works correctly' will appear wholly unrealistic for anyone with expertise in computer science or software engineering. That is because s69 demands a 'yes or no' – that is, a binary – answer to the question of whether a computer is working correctly or not and assumes that the answer is trivially easy to provide.[12] The reality is far more complex.[13] All computers have a propensity to fail, possibly seriously. All computer systems contain bugs, and some of these may rarely reveal themselves in any obvious or noticeable way, because they can masquerade as normal behaviour.

A particular computer system failure may very well have been caused by software, even if that software has previously been very reliable. While evidence of previous failure undermines a presumption of current proper functioning, certain kinds of failure that have never been seen before may still occur in the future, when a latent bug manifests itself for the first time.[14]

The fact that a computer has failed may well not be obvious. Even when a failure has been identified, it may be infeasible (that is, not possible) to discover whether it was caused by a software bug or improper operation. As a result, a person challenging evidence derived from a computer is unlikely to know what documents or records might show whether a relevant error has occurred, and so cannot request they be disclosed. They will typically not have been privy to the circumstances in which the system in question is known to fail or may have failed.

Practical proposal

We propose that the two-stage approach recommended by Paul Marshall and others is adopted when the reliability of computer evidence is challenged on reasonable grounds and where establishing its reliability is important to deciding the case. The proposal is simple and can be effective. It is designed to allow a party to justify why computer evidence can be relied upon, and to support the interests of justice while not imposing an undue or expensive burden on the parties. A *summary* of the proposal is set out below.[15]

In the first stage, the parties should perform a reasonable and proportionate search for documents that would assist the court in assessing the reliability of evidence, specifically:

1) records of known errors and bugs in the system, their effect, and the actions taken in response,

2) description of information security and other relevant standards and processes followed,

3) reports of audits performed on the system and how it is managed,

4) evidence showing that reports of errors are managed properly and that changes to the system are properly controlled,

5) evidence confirming that the search for

documents was performed adequately, and was done so by a person with appropriate authority and knowledge, and

6) assurance that reasonable steps have been taken to establish that the evidence presented has not been tampered with.

All the documents and records mentioned above are routinely kept or are readily available for all professionally developed and managed systems, so disclosure is not onerous. Furthermore, for many critical applications (e.g., healthcare IT), these documents will be *controlled documents*, dated, signed off, etc. To claim that such disclosure is onerous (given that computers can do it automatically) would implicitly call into question whether the party is managing the relevant documents adequately for the purposes of professional software development.

If the limited disclosure in the first stage identifies problems, including inadequate records or documentation, then a more detailed examination of evidence should be performed. This second stage would be necessary if the disclosed information:

1) shows that the system may not have been adequately managed,

2) shows that the number of bugs is sufficiently high to question the reliability of the system, or

3) identifies specific errors that provide grounds for questioning the evidence.

Authors: Nicholas Bohm (nbohm@ernest.net), James Christie (jameschristie2020@gmail.com), Peter Bernard Ladkin, Bev Littlewood (bevlittlewood@icloud.com), Paul Marshall (PMarshall@cornerstonebarristers.com), Stephen Mason (stephenmason@stephenmason.co.uk), Martin Newby, Steven J. Murdoch (s.murdoch@ucl.ac.uk), Harold Thimbleby (harold@thimbleby.net), and Martyn Thomas CBE (martyn@mctar.uk).

1. [2019] EWHC 3408 (QB), at http://www.bailii.org/ew/cases/EWHC/QB/2019/3408.html.
2. [2019] EWHC 3408 (QB), [968].
3. https://www.lawcom.gov.uk/document/criminal-law-evidence-in-criminal-proceedings-hearsay-and-related-topics/.
4. Paragraph 13.7 – 13.12.
5. Paragraph 13.13.
6. Paragraph 13.14.
7. *Holt v Auckland City Council* [1980] 2 NZLR 124, per Richardson J at 128.
8. Paragraph 13.18.
9. Paragraph 13.23.
10. *Bates v The Post Office Ltd (No 6: Horizon Issues) Rev 1* [2019] EWHC 3408 (QB).
11. This is discussed in detail in Stephen Mason and Daniel Seng, editors, *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), 5.132 – 5.142; 5.226 – 5.237, open source at https://humanities-digital-library.org/index.php/hdl/catalog/book/electronic-evidence-and-electronic-signatures.
12. James Christie, 'The Post Office Horizon IT scandal and the presumption of the dependability of computer evidence', *Digital Evidence and Electronic Signature Law Review* 17 (2020) 49–70, and Peter Bernard Ladkin, 'Robustness of software' *Digital Evidence and Electronic Signature Law Review* 17 (2020) 15–24, https://journals.sas.ac.uk/deeslr/issue/view/578.
13. *Electronic Evidence and Electronic Signatures*, Chapter 5.
14. Peter Bernard Ladkin, Bev Littlewood, Harold Thimbleby and Martyn Thomas CBE, 'The Law Commission presumption concerning the dependability of computer evidence', 17 *Digital Evidence and Electronic Signature Law Review* (2020) 1–14, at 13–14, https://journals.sas.ac.uk/deeslr/issue/view/578.
15. 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, at 23–25, https://journals.sas.ac.uk/deeslr/article/view/5240; see also 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/issue/view/584.