City Research Online

City St George's, University of London

Citation: Marshall, P., Christie, J., Ladkin, B., Littlewood, B., Mason, S., Newby, M., Rogers, J., Thimbleby, H. & Thomas, M. (2021). Recommendations for the probity of computer evidence. Digital Evidence and Electronic Signature Law Review, 18, pp. 18-26. doi: 10.14296/deeslr.v18i0.5240

This is the published version of the paper.

This version of the publication may differ from the final published version. To cite this item please consult the publisher's version.

Permanent repository link: https://openaccess.city.ac.uk/id/eprint/25410/

Link to published version: https://doi.org/10.14296/deeslr.v18i0.5240

Copyright and Reuse: Copyright and Moral Rights remain with the author(s) and/or copyright holders. Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge, unless otherwise indicated, provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way. For full details of reuse please refer to City Research Online policy.

City Research Online: http://openaccess.city.ac.uk/ publications@citystgeorges.ac.uk

ARTICLE:

Recommendations for the probity of computer evidence

By **Paul Marshall, James Christie, Peter Bernard Ladkin, Bev Littlewood, Stephen Mason, Martin Newby, Jonathan Rogers, Harold Thimbleby** and **Martyn Thomas CBE**

Every significant program contains many bugs[1] that will cause it to fail to produce correct results when some particular combination of input data is encountered.

This paper sets out recommendations for a two stage disclosure process[2] in an attempt to avoid the problems with disclosure of computer data/material in court proceedings, problems that have been exposed in two cases in England: the Post Office Horizon scandal, and the case of the nurses in *R v Cahill, R v Pugh*, both of which are discussed below.

Introduction

There exists widespread misunderstanding about the nature of computers and how and why they are liable to fail. The decision of the High Court in *Bates v Post Office Ltd Rev 1*[3] (*Horizon Issues*) implies that the present approach to the disclosure and evaluation of evidence produced by computers in legal proceedings is unsatisfactory.

The Post Office, as a private prosecutor, brought private prosecutions and secured resulting criminal convictions on the basis of data produced by the Horizon computer system. That system was held by Mr Justice Fraser to have been unreliable and lacking in robustness.[4] This was revealed in December 2019 as the outcome of group civil litigation that involved 557 claimants, and at a cost of several tens of millions of pounds. It is salutary that, but for that group civil litigation, the referral by the Criminal Cases Review Commission to the Court of Appeal of an unprecedented number of criminal convictions as possible miscarriages of justice would not have happened.[5]

The Criminal Cases Review Commission (CCRC) concluded, under its Statement of Reasons, that those concerned should not (in its view) have been convicted, given Fraser J's findings of fact about the unreliability of the Post Office Horizon computer system. In addition, the CCRC's view is that they should never have been prosecuted in the first place.

A common feature of the *Bates* case is that the convictions were based upon inferences drawn from data produced by the Horizon computer system. The inference was that the subpostmaster or subpostmistress in question *must have* taken (stolen) the money evidenced by a computer 'shortfall'. In this

[1] The term 'bug' means an error, flaw, mistake or fault in a software program or system. Drawing from the work of Professor Ladkin (Peter B. Ladkin, *On Classification of Factors in Failures and Accidents* (Report RVS-Occ-99-02), available at https://rvs-bi.de/publications/), it is possible to classify most software errors into the following non-exhaustive categories: human errors in coding and software development; software design or specification errors; unintended or unanticipated software interactions, input data flaws and deliberate errors caused by operators or hackers remotely.

[2] The recommendations are jurisdiction-neutral. 'Disclosure' is used throughout this paper, and expressly includes 'discovery'.

[3] [2019] EWHC 3408 (QB), at http://www.bailii.org/ew/cases/EWHC/QB/2019/3408.html

[4] The word 'reliable' is used throughout this paper and used in accordance with the precise meaning as it is used in Peter Bernard Ladkin, Bev Littlewood, Harold Thimbleby and Martyn Thomas CBE, 'The Law Commission presumption concerning the dependability of computer evidence', *Digital Evidence and Electronic Signature Law Review* 17 (2020) 1-14, https://journals.sas.ac.uk/deeslr/article/view/5143. See also Peter Bernard Ladkin, 'Robustness of software' *Digital Evidence and Electronic Signature Law Review* 17 (2020) 15-24, https://journals.sas.ac.uk/deeslr/article/view/5171.

[5] The Criminal Cases Review Commission's process for review of convictions relating to the Post Office and Horizon accounting system (Number 2020-0040, 3 March 2020), House of Commons Library, https://commonslibrary.parliament.uk/research-briefings/cdp-2020-0040/.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 4.0 International Licence

respect, a systemic problem is apparent, so far as defendants appear routinely to have been wrongly convicted on unsatisfactory evidence and incomplete computer records.

The material available to the CCRC to support the appeals only became available in the course of the group litigation in 2018-2019, almost 20 years after the first prosecutions by the Post Office for Horizon 'shortfalls' following the introduction of the Horizon system in 1999. The system was supplied by Fujitsu.

The Post Office disclosed error records for the first time in 2018. Fraser J found these records to be of central importance to his judgment on the most important of the preliminary issues: 'To what extent was it possible or likely for bugs, errors or defects of the nature alleged … to have the potential (a) to cause apparent or alleged discrepancies or shortfalls relating to Subpostmasters' branch accounts or transactions, or (b) undermine the reliability of Horizon accurately to process and to record transactions …'.[6] These documents included the 'Known Error Log' or 'KEL'. Fraser J in his judgment identified what he terms 'audit data',[7] also known as ARQ data.[8] This data was the best evidence of particular branch transactions that was available to the Post Office and was held centrally by Fujitsu. It is a remarkable feature of Fraser J's judgment that that data appears often not to have been obtained by the Post Office from Fujitsu. Fujitsu was contractually obliged to supply it to the Post Office. It appears an issue may have been cost, in so far as Fujitsu charged the Post Office to obtain access to that data. But, as Fraser J observed, cost is not a ground for important evidence not being obtained or disclosed.

The legal presumption of the reliability of computers

The present legal position is the result of the repeal of s. 69(1)(b) of the Police and Criminal Evidence Act 1984 by s. 60 of the Youth and Criminal Evidence Act 1999. The repeal was a response to the Law Commission recommendation in its paper *Evidence in Criminal Proceedings Hearsay and Related Topics* (1997 Law Com. No. 216).[9] Prior to its repeal, s. 69 provided that:

> (1) In any proceedings, a statement in a document produced by a computer shall not be admissible as evidence of any fact stated therein unless it is shown …
>
> > (b) That at all material times the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents.

PACE 1984 s. 69 subsection 1(b) represented a considerable imposition upon parties wishing to rely upon computer evidence. (The Civil Evidence Act 1968 included analogous provisions, repealed by the Civil Evidence Act 1995.)

In the absence of formal statutory requirements, as the Law Commission had suggested in its paper, the courts from 1999 have applied the *presumption* of the proper functioning of *machines* (for example, *Castle v Cross* [1984] 1 WLR 1372, [1985] 1 All ER 87, [1984] Crim LR 682) to computers. A full discussion of the Law Commission's recommendation, the repeal of s. 69(1)(b) and the resulting evidential *presumption* of the correct working of computers – and a justification for the claims made in this paper – is to be found in the article by Ladkin and others, *The Law Commission presumption concerning the dependability of computer evidence*.[10]

The *presumption* of the correct working of a computer is merely that. It is an *evidential* presumption that may be rebutted. The circumstances in which an effective challenge may be made such as to displace

[6] [2019] EWHC 3408 (QB) at [18].

[7] [2019] EWHC 3408 (QB), [906] 'Audit data is a complete and accurate record of everything that has occurred, which in the context of Horizon means including a full record of keystrokes used by a SPM (or assistant) in the branch. This accurate record is kept in what is called the audit store. This is a secure place for the keeping of such data. It is vital to the proper operation of a system such as Horizon that such accurate audit data is kept'; [919] 'audit data requests (also called ARQ requests)'.

[8] Note, Known Error Log (KEL) and Audit Data Requests (ARQ) were terms adopted and used by the Post Office and Fujitsu.

[9] The Law Commission paper was a response to a reference by the Secretary of State for the Home Department on 28 April 1994, the reference itself was in response to the Royal Commission on Criminal Justice.

[10] Peter Bernard Ladkin, Bev Littlewood, Harold Thimbleby and Martyn Thomas CBE, 'The Law Commission presumption concerning the dependability of computer

the presumption will inevitably vary. In principle, the threshold for rebutting the presumption so that the *onus of proof* is upon the party relying upon a document to prove it, and thus prove the integrity and reliability of its computer source (where otherwise hearsay), is low. Once the presumption is displaced, then the evidential burden (*onus of proof*) moves to the person seeking to rely upon evidence derived from a computer. That is to say, the evidential burden is to prove that the source of the evidence may be relied upon, so that the document in question may be accepted as evidence of the facts stated therein. In a criminal trial that burden is to the criminal standard.

Disclosure as a procedural problem

As a matter of procedure, the Post Office *Bates* litigation suggests that the *kind* of documents that (a) are likely to exist, and (b) ought to be disclosed as a matter of course, where data/documents generated by a computer system of any size are in issue, are possibly not generally well-understood or recognised.

It is a matter of surprise that important documentary records, such as the Fujitsu Known Error Log (KEL), were disclosed only in response to a direction from the court and in the face of opposition by the Post Office. These were disclosed by the Post Office in 2018. But as Fraser J noted, the KEL was 'a comprehensive record of the errors and defects of which Fujitsu had become aware over the life of the Horizon system'.[11] The vital importance of this evidence is identified at paragraph [559] of his judgment:

> 'There are certain categories or descriptions of classes of documents that have featured heavily in the evidence at the Horizon Issues trial. The path to disclosing them has not always been smooth. The majority, if not all, of the technical documents that relate to how Horizon was actually operating in fact in IT terms are in the possession of either the Post Office or (more usually) Fujitsu. The two most important categories, in my judgment, are Known Error Logs (also known as "KELs") and PEAKs. The first of these records or logs known errors, which means errors with the Horizon system. The latter is a browser-based software incident and problem management system used by Fujitsu for the Post Office account, in other words for incidents and problems associated with Horizon that occur.'

Fraser J found that the Post Office by its defence maintained a position on the KEL that was misleading and substantially wrong (paragraph [582]). In correspondence, the Post Office's solicitors questioned that the KEL records existed, a matter Fraser J found to be 'disturbing' (paragraph [577]). Thereafter, the Post Office contended by its counsel that the KEL was 'irrelevant' – a 'complete red herring' (paragraph [587]). In fact, the KEL was of fundamental importance to Fraser J's judgment on the principal preliminary issue of the Horizon system's reliability and propensity to fail in the way alleged by the claimants. When established that the KEL both (i) existed and (ii) was relevant, the Post Office's position was that the documents were not within its power to disclose (paragraph [605]) – a contention that Fraser J rejected.

Fraser J deals with related PEAK error records (a browser-based incident management system) and the manner of their disclosure by the Post Office at paragraphs [615]-[621] of his judgment. Two weeks before exchange of experts' reports for trial in March 2019, the Post Office disclosed 218,000 different PEAK error records.

Given the scale of the litigation, the Post Office's strenuous resistance to disclosing its Horizon computer error records and logs, most if not all of which appear not to have been disclosed in the many previous prosecutions by the Post Office of its subpostmasters and subpostmistresses and others, is a matter of concern.

Further, that for 18 years the Post Office appears not to have disclosed documents *routinely maintained and kept* for any computer system of any size and complexity, suggests that existing disclosure arrangements in legal proceedings do not work effectively, and in any event are inadequate to secure their intended purpose – fairness or 'equality of arms'.

evidence', *Digital Evidence and Electronic Signature Law Review* 17 (2020) 1-14, https://journals.sas.ac.uk/deeslr/article/view/5143

[11] [2019] EWHC 3408 (QB) at [610].

A significant problem arises when there is a serious imbalance in information and data available to a party. In many cases, no doubt, the kind of problem to which disclosure may be relevant in any given legal proceedings may be apparent from the factual circumstances. This may well not apply where an issue arises in connection with the reliability of a computer system, because the cause of failure may well not be obvious, as it was not obvious with the Post Office's Horizon computer.

Thus, where a person challenging evidence derived from a computer is required to identify the issue to which the disclosure is relevant, they may typically be unable to do so, because they will not have been privy to the circumstances in which the system in question is known to fail or to have failed. General or unfocussed disclosure requests tend to be rejected by the courts in these circumstances on grounds of their being 'fishing expeditions'. There is a risk, in such circumstances, of a party with access to relevant data and disclosable material being able to be obstructive and to avoid giving relevant disclosure.

This problem has been acknowledged by the European Court of Human Rights in the *Guide on Article 6 of the European Convention on Human Rights*, Right to a fair trial (criminal limb):[12]

> 'In the context of disclosure of evidence, complex issues may arise concerning the disclosure of electronic data, which may constitute a certain mass of information in [the] hands of the prosecution. In such a case, an important safeguard in the sifting process is to ensure that the defence is provided with an opportunity to be involved in the laying-down of the criteria for determining what might be relevant for disclosure'.

We agree. There is much to be said for rules of court providing for a collaborative approach for the disclosure of documents in this context - and to some extent a collaborative approach is already provided for in connection with disclosure of electronic documents more generally.[13] It is plainly unsafe and unsatisfactory for a defendant/objector to be required to identify the specific issue to which disclosure is said by them to be relevant. Such a requirement, as noted, will frequently be impossible for a defendant to comply with.

Presuming the correct working of computers – an unsafe presumption?

While the convenience that was sought to be achieved by repeal of s. 69(1)(b) of the Police and Criminal Evidence Act 1984 is understandable, a presumption that a computer 'works correctly' in itself is unsafe and, for anyone with expertise in the area, will appear wholly unreal, because it suggests a binary question of whether the computer is working or not.[14] The reality is more complex.[15] All computers have a propensity to fail, possibly seriously. That is to say, they have a latent propensity to function incorrectly.

A program on a mobile telephone might hitherto have contained tens of thousands of lines of software code. A program such as Horizon will contain tens of millions of lines of code, and will be exceedingly complex. Programming is a human task and programmers make mistakes; an error rate in writing software code of 10 errors per thousand lines of code

[12] (August 2020), paragraph 166, at https://www.echr.coe.int/documents/guide_art_6_criminal_eng.pdf.

[13] *The Attorney General's Guidelines on Disclosure for investigators, prosecutors and defence practitioners* (2020) (not in force at the time of writing) is a step in the right direction in respect of electronic material, for which see paragraphs 54-57, and in which the overriding obligation to ensure a fair trial is stressed (paragraph 55), available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/923774/Attorney_General_s_Guidelines_on_Disclosure_2020_NOT_YET_IN_FORCE.pdf.

[14] 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, https://journals.sas.ac.uk/deeslr/article/view/5226 and Peter Bernard Ladkin, 'Robustness of software' *Digital Evidence and Electronic Signature Law Review* 17 (2020) 15-24, https://journals.sas.ac.uk/deeslr/article/view/5171.

[15] Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017), Chapter 6, https://humanities-digital-library.org/index.php/hdl/catalog/book/electronicevidence (the 5th edition is to be published in 2021).

is considered good, 1 error per thousand lines is rarely if ever achieved.

To give an example, McDermid and Kelly reported that the 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],[16] and determined that it contained about 1.4 safety- critical faults per kLoC[17] (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.')[18] 'Safety- critical faults' means faults whose possible consequences include system failures causing damage including injury or death and/or damage to the environment.[19]

Further, computers of any complexity often interact with other systems. Such interfaces create complexity and augment the risk of failure (as found, for example, in the frequent problems/failures encountered with the 'Riposte' communication platform in the 'Legacy Horizon' version of the system that the Post Office operated until 2010).

It follows from the discussion above that every significant program will contain many bugs that will cause it to fail to produce correct results when some particular combination of input data is encountered.

It is the presence of software bugs that can determine the *reliability* of a system, measured, for example, in terms of the frequency with which it will fail during operation. (Environmental conditions and cybersecurity issues can also affect a system and result in faults and failures.)

It is known that the effect of bugs upon system reliability can vary enormously, some of them will be seen very rarely, perhaps never in the lifetime of the system. Others will occur more frequently and thus contribute more to unreliability. Further, bugs by their nature can vary greatly in the seriousness of the failures that they induce.

During the development of a software system, some bugs will be detected and removed – for example, by testing. There are statistical (and other) techniques that allow this kind of information to be used to draw inferences about the bugs that remain when the system is put into operation. It is the remaining/unresolved bugs and their effects that will determine the reliability of the system.

As a system is used, more will be learned about its reliability. However, even for a system that has so far been reliable in use, it cannot be presumed that when a failure occurs this is not a result of a software bug. That is to say, the absence of evidence of failure is not equivalent to evidence of absence of bugs – a misconception that appears in the Post Office prosecutions and in the Post Office's evidence in the *Bates* litigation. This misunderstanding is closely related to the common misapprehension that computer errors will be apparent to an operator (see below).

Common false perceptions and beliefs

The Law Commission, in its review of the law on hearsay evidence in *Evidence in Criminal Proceedings: Hearsay and Related Topics* (1997), under Part XIII 'Computer Evidence', suggested that 'most computer error is either immediately detectable or results from error in the data entered into the machine'.[20] It is true that an error that causes a system crash is usually immediately detectable, and also true that the behaviour of a computer system is determined by data entered into the machine at some point in the past. It is, however, wrong to conclude that every, or even most, erroneous output from a computer will have been caused by the user affected by it. Further, it is not true that most computer system failures will be detectable by the user of the system. The latter proposition is of particular importance. In decided

[16] RTCA/DO-178B, Software Considerations in Airborne Systems and Equipment Certification, December 1, 1992.
[17] Thousand lines of code.
[18] John McDermid and Tim Kelly, Software in Safety-Critical Systems: Achievement and Prediction, Nuclear Future 02(03), 2006, 3.1. Preliminary version is available at https://www-users.cs.york.ac.uk/tpk/inuce2004.pdf.
[19] See: *The Law Commission presumption concerning the dependability of computer evidence*.

[20] Professor Colin Tapper in 'Discovery in Modern Times: A Voyage around the Common Law World' (1991) 67 Chicago-Kent Law Review 217, 248 cited by the Law Commission in its 1997 paper at paragraph 13.7.

cases there is some support for this popular, though erroneous, view, for example: *DPP v McKeown and Jones* [1997] 1 WLR 295, 301C-D and *R v Governor of Pentonville Prison Ex p Osman (No 1)* [1990] 1 WLR 277, 306H. The proposition is known to have been relied upon by the Post Office in prosecuting its sub-postmasters. The perception and commonly held belief is wrong. Mr Justice Fraser addressed this issue in his *Horizon Issues* judgment:

> '[972] Did the Horizon IT system itself alert Subpostmasters of such bugs, errors or defects as described in (1) above and if so how?
>
> [973] Answer: Although the experts were agreed that the extent to which any IT system can automatically alert its users to bugs within the system itself is necessarily limited, and although Horizon has automated checks which would detect certain bugs, they were also agreed that there are types of bugs which would not be detected by such checks. Indeed, the evidence showed that some bugs lay undiscovered in the Horizon system for years. This issue is very easy, therefore, to answer. The correct answer is very short. The answer to Issue 12 is "No, the Horizon system did not alert SPMs". The second part of the issue does not therefore arise.'

The Post Office prosecutions are by no means the only instances where the failure to recognise the possible unreliability of computer evidence/data has led to serious miscarriages of justice.

In *R v Cahill, R v Pugh*,[21] the court was concerned with alleged wilful neglect (possibly as serious a charge as can be made against a healthcare professional), a view that, it transpired, was based on the mistaken interpretation of corrupt NHS patient data. Professor Harold Thimbleby, one of the authors of this paper, was an expert witness in the case. In a subsequent paper, Thimbleby commented: '… The broader problem is the uncritical acceptance of IT, from legal, regulatory, procurement and other perspectives… . …[N]obody seems to be fully aware of the complexity and risks of IT. This results in lax legislation, lax regulation and lax procurement, and, in turn, lax manufacturing since no useful standards of quality can be demanded by hospitals. Unawareness, in turn, results in lax management, and, unnoticed inconsistencies between clinical care and its unreliable monitoring'.[22] The 73 nurses subject to disciplinary proceedings were, presumably, conscientious healthcare professionals whose lives were turned upside-down by misunderstood and unreliable computer data that was uncritically accepted.

Recommendations

The dilemma is that all computer systems can and are likely to fail, and thus produce erroneous output. However, insufficiently specific applications – 'fishing expeditions' – for disclosure of computer data are discouraged by the court (not least on grounds of being wasteful). The question arises as to how the courts can balance and resolve these considerations, that point in opposite directions so far as the disclosure of material is concerned.

The starting position will, of course, remain that disclosure, whether in civil or criminal proceedings, will be of material that is recognised to adversely affect the disclosing party's case or, alternatively, assist the case of the opposing party (or is otherwise relied upon by the disclosing party).

It is beyond the scope of the recommendations below to elaborate how data should be disclosed, other than to note that the mere disclosure of 'data' is not sufficient if it is not adequately defined for the purpose. For example, if data is encrypted, data has been disclosed, but it is not usable (technically, may not be 'inspected') until further details (in this case a decryption keyword) are provided.

Where the reliability of computer data is challenged on reasonable (as distinct from fanciful) grounds, it is suggested that a two-stage approach can be adopted. (A relevant consideration in the court's approach to disclosure should be whether the data or evidence in question is the only evidence or is otherwise of critical importance, as typically it was in the Post Office prosecutions.)

[21] 14 October 2014, at Cardiff Crown Court (T20141094, T20141061). The judge's ruling was published in the *Digital Evidence and Electronic Signature Law Review* 14 (2017) 67-71, https://journals.sas.ac.uk/deeslr/article/view/2541.

[22] Harold Thimbleby, 'Misunderstanding IT: Hospital cybersecurity and IT problems reach the courts', *Digital Evidence and Electronic Signature Law Review* 15 (2018) 11-32, https://journals.sas.ac.uk/deeslr/article/view/4891.

Stage 1

(i) As a matter of procedure, disclosure should be given of:

> (a) Known bugs in the system that have been reported, and the actions taken in response. This should include the disclosure of known error logs,[23] release notices,[24] change logs[25] and similar documents.
>
> (b) The party's information security standards and processes. This should extend to cover logical access controls[26] (including emergency access), security vulnerability notifications[27] and security patches.[28]
>
> (c) Relevant audits of systems and the management of the installation to provide assurance that suitable standards and processes have been implemented and complied with.
>
> (d) Evidence of reliably managed records of error reports and system changes, including evidence to demonstrate that basic precautions such as digital signatures have been implemented to detect and limit accidental or deliberate corruption.

(ii) The disclosure set out above should be provided by a person authorised to do so by the party subject to the disclosure obligation. The party with the disclosure obligation should be required to undertake a reasonable and proportionate search for the documents and records in question. Disclosure should be supported by evidence confirming that a reasonable and proportionate search has been undertaken by a person with appropriate authority and knowledge, and that:

> (a) The records disclosed are believed to be the records of the relevant standards, processes and audits, and of the known defects, security vulnerabilities, fixes and changes in the system.
>
> (b) The party seeking to rely upon the evidence in question has taken reasonable steps to satisfy itself that access to the system is controlled in such a way that unauthorised and undetected amendment of system data, in a way that might affect the evidence in question, is prevented.[29]

(iii) The disclosure exercise should, where possible, be collaborative and co-operative between the parties, rather than adversarial. In particular:

> (a) The parties should, if possible, seek to agree that the disclosed data is in a form that takes into account that the party to whom the disclosure is made should be able to conveniently read/use it.
>
> (b) It should not be required that the party challenging the reliability of the data relied upon should identify the particular issue to which the disclosure required to be given is alleged to go.

(iv) The documents under Stage 1 will be routinely kept and easily available for a bespoke system professionally developed and managed. The absence of such records will ordinarily suggest poor quality software/system management. For commercial-off-the-shelf software it should be enough to provide

[23] Records of the errors that have been reported in a system and what action was taken. This should include evidence of testing after each system change to ensure that the same error has not been reintroduced.

[24] Documentation of the changes that have been made in each new release of the software, including identifying all the known errors that have been corrected.

[25] Records of every change that has been made to the software (containing information about what was changed, what was affected, and what the results were, together with any resulting problems), including by whom, when and why it was done.

[26] Organisational processes and software controls that ensure data and systems can be read, changed, created and deleted only by people who have been properly authorised and identified.

[27] Notifications of a vulnerability in a software product that could allow unauthorized access to the system to compromise the integrity, availability, or confidentiality of an organisation's systems or data.

[28] Software changes to correct security vulnerabilities, often made to software systems between releases of the software because an error has been detected that is too important to wait for a new system release to correct it.

[29] The issue of remote access by a third party to Horizon branch terminals was a major issue in the Post Office *Bates* litigation. The fact that such access was possible was only conceded by the Post Office in January 2019. It had in fact been practiced from early after the introduction of the Horizon system in 1999. Fraser J considered the issue to be of central importance. Until 2010 no records were kept by Fujitsu of such actions.

evidence of the particular version and release of the software and to disclose release documentation (usually publicly available from the supplier) for the relevant version and subsequent releases. (The latter will reveal errors in the version in question later found and corrected.) In either case, proportionate Stage 1 disclosure should not be onerous, and for a professionally managed system should be a straightforward exercise.

Stage 2

(i) If the limited disclosure under Stage 1 reveals any one or more of the following:

> (a) a level of recorded defects or failures sufficiently high to provide grounds for questioning the reliability of the computer system from which the material is derived;
>
> (b) that there exist records of specific defects or failures that provide grounds for questioning the evidence sought to be relied upon;
>
> (c) that a person seeking to rely upon the evidence in question is not able to demonstrate that it has adequate control over the systems or data,

then the party seeking to rely upon the evidence produced by the computer system in question should be required to prove that none of the facts or matters identified under (a)-(c) above might affect the reliability of the material sought to be relied upon.

(ii) It is known that all large computer systems contain bugs, and that some of these may be 'small' bugs that reveal themselves rarely. This is true even for those systems that have been shown convincingly to be very reliable. It follows that, even in the case of such a reliable system, the court should have regard to the possibility that an apparent failure may be the consequence of a bug manifesting itself.[30] *Evidence of reliability is not evidence of the absence of software bugs*. The court should consider what degree of doubt remains in the context of all the other available evidence.

Concluding comment

It is likely that the procedural and evidential safeguards of the kind discussed, that might readily be provided under the rules of court, would have avoided the disastrous repeated apparent miscarriages of justice over the past 20 years. (Nevertheless, even with those procedural safeguards, the miscarriage of justice may not be altogether avoided.) Those apparent miscarriages of justice have occurred since the repeal of s. 69(1)(b) of the Police and Criminal Evidence Act 1984 in April 2000[31] for the reasons given by Mr Justice Fraser in *Bates v Post Office Ltd Rev 1*.[32] But for that group litigation, the fact of the fundamental unreliability of the Post Office's Horizon computer system would not have been revealed.

© Paul Marshall, James Christie, Peter Bernard Ladkin, Bev Littlewood, Stephen Mason, Martin Newby, Dr Jonathan Rogers, Harold Thimbleby and Martyn Thomas CBE, 2020

Paul Marshall, Barrister, Cornerstone Barristers, 2-3 Gray's Inn Square, Gray's Inn

James Christie, independent testing consultant with 35 years' IT experience as a system developer and designer, business analyst, IT auditor, project manager, test manager and information security manager

Peter Bernard Ladkin, Professor i.R. of Computer Networks and Distributed Systems, Bielefeld University and CEO of tech-transfer companies Causalis Limited and Causalis Ingenieurgesellschaft mbH

Bev Littlewood, Emeritus Professor of Software Engineering, Centre for Software Reliability, City, University of London

Stephen Mason, Barrister

Martin Newby, Emeritus Professor of Statistical Science, City, University of London

[30] For which see Peter Bernard Ladkin, Bev Littlewood, Harold Thimbleby and Martyn Thomas CBE, 'The Law Commission presumption concerning the dependability of computer evidence', *Digital Evidence and Electronic Signature Law Review* 17 (2020) 1-14, https://journals.sas.ac.uk/deeslr/article/view/5143.

[31] Repealed on 14 April 2000 by the Youth Justice and Criminal Evidence Act 1999 ss. 60, 67(3), Sch; Youth Justice and Criminal Evidence Act 1999 (Commencement No 2) Order 2000, art 2(c), Sch.

[32] [2019] EWHC 3408 QB.

Dr Jonathan Rogers, University Lecturer in Criminal Justice, Faculty of Law, Cambridge University, Fellow of Fitzwilliam College, co-Deputy Director of the Cambridge Centre for Criminal Justice, co-Director of Criminal Law Reform Now Network

Harold Thimbleby, Professor and See Change Digital Health Fellow, Swansea University, Wales, and Visiting Professor, UCL, London, Emeritus Professor, Gresham College, London

Martyn Thomas CBE, Emeritus Professor, Gresham College, London and Visiting Professor of Software Engineering at Aberystwyth University, Wales