BCS' response to the Ministry of Justice Call for Evidence: use of evidence generated by software in criminal proceedings

April 2025

Compiled by Martin Cooper, BCS Senior Editor, Policy and Content

Table of Contents

Executive Summary

BCS, The Chartered Institute of IT, believes that the current common law (rebuttable) presumption relating to computer evidence should be changed so it is fit for purpose in the modern era. As the Post Office scandal showed, proving that the computer was wrong is a near-impossible challenge.

However, we don't believe the burden of proof should be reversed, leaving the prosecution to prove the computer was functioning correctly before evidence can be accepted. Reinstating Section 69 (or similar) isn't the answer.

Instead, BCS proposes a compromise position based on two tests proposed by the authors *Marshall et al in Digital Evidence and Electronic Signature Law Review*: [1]

Stage 1: Perform a reasonable and proportionate search for documents that would assist the court in assessing the reliability of the evidence. This includes records of known errors, information security standards, audit reports, and evidence of proper error management.

Stage 2: If Stage 1's limited disclosure finds issues like bugs or errors that question the evidence, then the party seeking to rely on that evidence should prove how those uncovered issues might affect the evidence.

The response to the call for evidence was written by Dr Sam De Silva, a Fellow and Chartered senior member of BCS, who specialises in technology law.

He is a practicing solicitor and Partner and Global Co-head of the Commercial Practice Group at the international law firm, CMS Cameron MacKenna Nabarro Olswang LLP specialising in technology law.

He is also the Chair of BCS' Law Specialist Group, one of over 50 BCS specialist interest groups. Since 2021 he, and BCS, have **called for an end to the legal presumption that data from computer systems is always correct, with no burden on the prosecution to prove** it.[2]

In addition, further contributions were provided by the BCS Fellows Technical Advisory Group (F-TAG) – a panel of experts who analyse technology trends and assess their impact on the digital industries, as well as on the UK economy and society.

For more information contact Dan Howl, BCS Head of Policy: Dan.Howl@bcs.uk

[1] Marshall, P., Christie, J., Ladkin, P.B., Littlewood, B., Mason, S., Newby, M., Rogers, J., Thimbleby, H. and Thomas CBE, M. (2020). Recommendations for the probity of computer evidence. *Digital Evidence and Electronic Signature Law Review*, pp.18–26. doi:https://doi.org/10.14296/deeslr.v18i0.5240.

[2] https://www.computerweekly.com/news/252501510/BCS-demands-reform-to-rules-on-computer-evidence-following-Post-Office-Horizon-scandal-revelations

Call for Evidence Questions:

Question 1: The current common law (rebuttable) presumption is that computers producing evidence were operating correctly at the material time.

The presumption that computer-generated evidence is inherently reliable is increasingly unfit for purpose in modern criminal prosecutions. Unfortunately, the Post Office Horizon scandal illustrates this point. Hundreds of sub-postmasters were wrongly convicted based on data from a computer system later found to be error-prone and unreliable.

As Dr De Silva explained in an article for BCS in 2024[3], the presumption that a computer is 'working properly' is wholly unrealistic for anyone with computer science or software engineering expertise. It requires a binary answer — a 'yes or no' as to whether a computer is working correctly or not. The assumption assumes that the answer is easy to give.

The reality is, of course, far more complex. All computers have a propensity to fail, possibly seriously. All computer systems contain bugs, errors or defects, and some of these may rarely reveal themselves in any obvious or noticeable way because they can masquerade as normal behaviour.

How easy or difficult do you believe it is at present for this presumption to be effectively rebutted?

At present, rebutting the presumption of computer evidence is exceptionally difficult. Although the evidential burden theoretically shifts to the party relying on the computer-generated evidence once the presumption is challenged, the process is hampered by the technical intricacies of digital systems.

It has been shown that defendants in cases like Horizon have struggled to access crucial system logs, error reports, and documentation that could undermine the assumed reliability of the evidence. Additionally, some of the lower courts often lack the specialised technical expertise required to scrutinise complex software and digital data, meaning that challenges to the reliability of computer evidence must overcome both procedural and substantive hurdles that favour the status quo.

What barriers do you see in effectively rebutting this presumption?

1) There is a significant disclosure problem. Key documents, such as known error logs and audit trails, are often not provided by the prosecution until compelled by the court, as seen in the delayed disclosure in the Horizon litigation.

[3] Bcs.org. (2024). *Post Office scandal: understanding computer evidence in cases*. [online] Available at: https://www.bcs.org/articles-opinion-and-research/post-office-scandal-understanding-computer-evidence-in-cases/.

2) There is an inherent technical barrier, as most legal professionals and judges lack the expertise necessary to evaluate sophisticated computer systems' inner workings and potential flaws.

Released in around 2002, Fujitsu's Horizon software had over 3.5 million lines of code , and history shows how hard it was for the Postmasters to demonstrate that the ill-fated system had bugs[4]. For context, an average car needed around 100 million lines of code in 2015, and this doubled by 2020. With more automation inbuilt, today's most sophisticated cars might have around 650 million lines of code.

Modern software also presents another challenge to a legal team looking to find, reproduce and challenge errors. Software isn't like a book—it doesn't read from chapters one to 12. Instead, software is non-linear. Imagine reading a book where chapters and even paragraphs have been shuffled.

To add yet more complexity, software systems are often systems of systems. Multiple outputs from one system become multiple inputs to another. Returning to our book analogy, you'll need to read all three parts of the trilogy and understand how they interlink at multiple points. To complicate things further, each of these interdependent parts could be written in a different programming language, potentially by a different person and at a different time. Each part may even run concurrently and on a different computer.

If that's not enough, commercial software—unlike a book—often evolves. Software teams often look to fix bugs and add new features, which means different versions will exist.

Considering all this, finding evidence of flaws in software systems is a painstaking and expensive job that requires considerable professional and technical experience.

3) Resource constraints play a critical role. Individuals and defendants typically lack the financial and technical resources to hire independent forensic experts who can provide the necessary evidence to contest the reliability of digital records.

Question 2: Can you provide examples from other jurisdictions or situations where software reliability must be certified?

There are undoubtedly many industries and situations where software reliability must be certified. Certification is critical in ensuring that software systems protect people from harm. As such, it is easy to imagine that mandating certification could be a silver bullet to keeping the public safe and making it easier for courts to deal with software-based evidence. Putting our faith entirely in certification is, however, not the entire solution.

We are aware of the following examples where software certification exists, and there may be others:

[4] https://www.jfsa.org.uk/

- **Medicines and Healthcare**: The Yellow Card scheme is run by the Medicines and Healthcare Products Regulatory Agency (MHRA)[5], which safeguards the quality and efficacy of medicines, vaccines, medical devices, blood products, and e-cigarettes in the United Kingdom. Although medication interactions are the most common, medical device reporting (including software issues) for regulated devices can be reported via this route for monitoring.
- **Aerospace:** The UK's Civil Aviation Authority (CAA) uses software certification to ensure that aviation systems meet stringent safety and security standards. [6]This process helps mitigate risks associated with cyber threats and vulnerabilities, ensuring that aircraft and related systems are resilient against unauthorised access and potential cyber-attacks.
- **Nuclear:** The UK's Office for Nuclear Regulation (ONR)7 uses software certification to ensure that safety-critical software for nuclear reactors meets rigorous standards. This process helps to maintain the highest levels of safety and security, minimising the risk of software-related failures that could impact nuclear operations

While often very rigorous, certification processes do not guarantee absolute faultlessness; they merely indicate that a product has been developed against a set of standards and that, when the code is in operation, it meets predefined criteria under specific conditions.

In summary, **certification regimes cover the software development process and, separately, how those software products perform** in the real world. However, **in the opinion of BCS, this misses a critical factor: people.**

BCS believes that requiring software engineers to be certified professionals can enhance software reliability and safety. These certified professionals would be accountable for ensuring the software has been developed to the correct certification standards.

We consider that ensuring that the software, the development process, and the professionals involved are all certified can significantly bolster the reliability of computer-generated evidence.

[5] Medicines and Healthcare products Regulatory Agency (2021). *The Yellow Card Scheme: Guidance for Healthcare professionals, Patients and the Public*. [online] Gov.uk. Available at: https://www.gov.uk/guidance/the-yellow-card-scheme-guidance-for-healthcare-professionals.
[6] https://www.caa.co.uk/commercial-industry/cyber-security/cyber-security-certification/
[7] Office (2024). *Office for Nuclear Regulation*. [online] Office for Nuclear Regulation. Available at: https://www.onr.org.uk/publications/regulatory-reports/other-reports/licensing-of-safety-critical-software-for-nuclear-reactors/ [Accessed 20 Feb. 2025].

- **Certified professionals are accountable** for ensuring the software has been developed to the correct certification standards, which enhances the reliability and safety of the software.

- **Certification acts as a foundational layer of trust,** providing a structured assurance that the software has been developed and maintained according to rigorous standards.

- **Certified professionals play a crucial role in this process** by adhering to these standards and ensuring that all development practices meet the required criteria. This, in turn, supports the first stage of the proposed two-stage disclosure process (see our response to Question 3 below) by offering a documented audit trail of compliance and quality control.

- **Certified professionals ensure that comprehensive records such as error logs, security patches, and system audits are meticulously maintained and disclosed**, facilitating a thorough and transparent evaluation of the software's reliability. When software systems and their development processes are certified, it becomes easier to disclose comprehensive records such as error logs, security patches, and system audits, thereby facilitating a thorough and transparent evaluation of the software's reliability.

This alignment with certification standards not only supports in meeting the disclosure requirements but also sets a robust groundwork for the subsequent independent technical validation, as outlined in the response to question 3. By integrating certification into the framework, we consider the credibility and reliability of computer evidence can be enhanced.

Question 3: If the position were to be amended, what, in your opinion, would be the most appropriate and practicable solution given our aims and objectives set out above

Where the reliability of computer data is challenged, we suggested that a two-stage approach proposed by the authors Marshall et al in Digital Evidence and Electronic Signature Law Review can be adopted: [8]

[8] Marshall, P., Christie, J., Ladkin, P.B., Littlewood, B., Mason, S., Newby, M., Rogers, J., Thimbleby, H. and Thomas CBE, M. (2020). Recommendations for the probity of computer evidence. *Digital Evidence and Electronic Signature Law Review*, pp.18–26. doi:https://doi.org/10.14296/deeslr.v18i0.5240.

- **Stage 1:** Disclosure should cover reported bugs, error logs, release notices, and change logs, along with information security standards, logical access controls, vulnerability notifications, and security patches. It should also include relevant system audits and management practices and evidence of managed error reports and system changes, including digital signatures to detect and limit corruption. Disclosure must be authorised by a person with appropriate authority and knowledge, and it should be thorough and collaborative to ensure that data is accessible and reliable. The absence of such records typically indicates poor management. The disclosure process should also be reasonable and proportionate, ensuring the disclosed data is usable for the receiving party.

- **Stage 2:** If Stage 1 disclosure reveals significant defects or failures in a computer system, the party relying on the system's evidence must prove these issues don't affect reliability. All large systems have bugs, even reliable ones, so courts should consider that apparent failures might be due to bugs. Evidence of reliability doesn't mean there are no bugs. Courts should weigh the degree of doubt alongside other evidence.

In summary, a trial of the computer evidence should precede the trial of the case itself. Such an independent evaluation would serve as a “trial of the evidence,” ensuring that only correctly vetted digital data is used to substantiate claims. To make this safeguard effective, procedural rules should set out the disclosure obligations and the criteria for assessing the evidence, thereby shifting the burden of proof from the defendant to the party relying on the evidence.

If expert witnesses are required—whether jointly or singly instructed—their expertise should span digital forensics, software engineering, and systems reliability. They should hold recognised qualifications such as Chartered IT Professional (CITP) or Chartered Engineer status and have demonstrable experience with forensic analyses of complex software systems.
While there is a current pool of such experts, maintaining a sufficient number will likely require ongoing professional development and possibly creating a dedicated accreditation or training program to keep pace with rapidly evolving technology.

In summary, replacing the current presumption with a system that mandates full disclosure and independent technical validation—supported by regular oversight and the involvement of highly qualified experts—provides an effective, future-proof, and operationally practical solution for addressing the reliability of computer evidence in modern criminal prosecutions.

Question 4: In your opinion, how should ‘computer evidence’ for these purposes be best defined.

The definition of “computer evidence” should encompass the following key elements:

- **Digital Origin:** Computer evidence should be defined as any data or information that is created, stored, transmitted, or manipulated by a computer or digital device. This includes, but is not limited to, data from personal computers, servers, mobile phones, tablets, and other digital devices.

- **Electronic Data:** The term should cover all forms of electronic data, including text documents, emails, databases, spreadsheets, digital images, audio and video files, and metadata. It should also include data from social media platforms, cloud storage, and other online services.

- **Software-Generated Evidence:** The definition should explicitly include evidence generated by software applications, such as logs, transaction records, and automated reports. This also encompasses data produced by specialised forensic software used in the investigation and analysis of digital evidence.

- **Chain of Custody:** The definition should require a clear and documented chain of custody for the evidence, detailing how it was collected, preserved, and handled. This is crucial for establishing the reliability and credibility of the evidence.

- **Expert Testimony:** Given the technical nature of computer evidence, the definition should acknowledge the necessity of expert testimony to explain the methods used to collect, analyse, and interpret the data. Experts should be qualified and their methodologies should be widely accepted within the relevant field.

Computer evidence should not merely be viewed as the content of digital records but also encompass the mechanisms through which such records are created, stored, and maintained.

BCS agrees that software-generated evidence should be within scope, while evidence merely captured or recorded by a device should be considered out of scope.

The rationale for this distinction is that computer-generated evidence inherently depends on the proper functioning of the software that creates it.

In contrast, data captured or stored—such as a scanned document, a photograph, or a video recording—does not typically depend on complex software logic for its validity.

The risk of errors affecting the reliability of stored information is lower than that associated with software-generated data.

Question 5: Are there any other factors you believe are important for us to consider?

It's impossible to discuss software without mentioning artificial intelligence. And if the law of evidence remains as it is, AI will likely make the lives of courts, defence teams and prosecutors much harder.

AI-generated outputs are often the result of incredibly complex processes based on vast amounts of data and highly complicated algorithms. The complexity of these systems makes it hard to explain how they work (i.e. the "black box" problem) – even for the computer scientists who are experts in AI.

In a court setting, this lack of transparency would make it very hard to prove that the resulting evidence was correct, had not been tampered with, and not generated based on biased data.

The lack of transparency and explainability in AI algorithms can affect the admissibility of AI-generated evidence in legal contexts, as courts require clear reasoning behind evidence. Rapid advancements in AI technology challenge legal systems to keep up, making it difficult for practitioners to handle and interpret AI-generated evidence.

This situation raises concerns about the authenticity of evidence, increased litigation costs due to the need for forensic experts, the ability of juries to distinguish real from fake evidence, and the potential for courts to be overwhelmed with AI-related cases.

In the EU this may not be as problematic as it seems. Under the EU AI Act,[9] providers and deployers of so-called 'high-risk' AI systems will be subject to significant regulatory obligations from 1 August 2026 when the obligations on high-risk AI systems listed in Annex III of the EU AI Act become applicable , with enhanced thresholds of diligence, initial risk assessment and transparency.

In addition, Annex III of the EU AI Act includes examples of AI systems used in a law enforcement context that are considered 'high-risk' AI systems. These include AI systems intended to be used to assess individuals' risks of offending or re-offending. It also covers AI systems used to evaluate the reliability of evidence in criminal investigations or prosecutions, or for profiling individuals in the course of detection, investigation or prosecution of criminal offences.

Who we are

BCS is the UK's Chartered Institute for Information Technology. The purpose of BCS as defined by its Royal Charter is to promote and advance the education and practice of computing for the benefit of the public.

[9] https://artificialintelligenceact.eu/the-act/

We bring together industry, academics, practitioners, and government to share knowledge, promote new thinking, inform the design of new curricula, shape public policy and inform the public.

As the professional membership and accreditation body for Information Technology we serve over 70,000 members including practitioners, businesses, academics, and students, in the UK and internationally. We also have over fifty specialist groups

We also accredit the computing degree courses in over ninety universities around the UK. As a leading information technology qualification body, we offer a range of widely recognised professional and end-user qualifications.

BCS
The Chartered Institute for IT
3 Newbridge House,
Newbridge Square,
Swindon SN1 1BY
BCS is a registered charity: No 292786