Response to the Ministry of Justice's "Use of evidence generated by software in criminal proceedings: Call for Evidence"[1]

Harold Thimbleby, 15 April 2025
Email: harold@thimbleby.net

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

(a) Is this Presumption fit for purpose in modern criminal prosecutions?

No.

(i) Please specify why you gave this answer

NASA's Voyager 1 spacecraft was launched in 1977. It has been sending computer evidence back to Earth ever since, such as stunning images of Saturn and its moons. Voyager has now been working continuously for nearly half a century, has flown far beyond the solar system, and is *still* sending reliable computer evidence back to us. NASA did professional engineering work to ensure Voyager works as planned. With good engineering, then, Voyager 1 shows we can have reliable computer evidence if we want it.

Note that the computer evidence reliability demonstrated by Voyager 1 is not just the reliability of the "trivial" Voyager on-board computer systems, but of all the highly sophisticated world-wide communications and data analysis systems, including the generation of the final high-quality images and videos distributed as reliable evidence about our solar system and the harsh environment beyond it.

Unfortunately, the rest of the world — with access to generally far less technical maturity and awareness than NASA — is unable to generate, manage, or have access to reliable computers and skilled users, and therefore are unable to create or manage reliable computer evidence.

A large part of the problem is that most people believe computers are reliable or reliable enough, so little or no effort (whether regulatory or technical) is put into ensuring the quality of computer systems, or for ensuring their programmers and operators are as well qualified as is evidently required at NASA and in other highly technical areas such as nuclear power.

Unlike every other technology, we routinely accept computers and software that needs regular updates and fixes. We are increasingly seeing a clash with computer culture and traditional culture as conventional products like cars and televisions now have embedded computers and need regular updates to fix bugs and introduce new features just to continue being used.[2]

[1] https://www.gov.uk/government/calls-for-evidence/use-of-evidence-generated-by-software-in-criminal-proceedings/use-of-evidence-generated-by-software-in-criminal-proceedings-call-for-evidence, 21 January 2025.

[2] One reason for the success of the Cloud is that it enables industry to force subscriptions as an income stream fixing bugs, when previously users could buy software outright. In terms of reliable evidence, because of continual updates the Cloud means that the precise version of software used to generate or process evidence may not be known.

While buying a new mobile phone every year might be seen as a benefit of innovation, the converse side is that industry no longer bothers to make reliable systems with a long lifetime, since consumers do not want to keep obsolete products and are happy to subscribe to software updates that conceal the poor quality of the original software.

In the mid-nineteenth century, Parliament passed the *Medical Act 1858* in response to the scandal that people were being treated by 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." Some quacks were deliberately cheating patients; but most were *unconsciously incompetent* and out of their depth. They did not know what they did not know. Without the need for qualifications, they and their employers had no awareness of just how incompetent they were. The Act fixed those problems, creating a rigorous framework of certification that survives to this day and which continues to adapt to innovations in healthcare.

Computers today are embedded in every area of modern life, including in courts. Although there are regular computer evidence scandals, and although there are regular computer failures, such as failed Government IT contracts and regular destructive cyberattacks and computer outages — *there is still no effective regulation for computer system performance, or certification for computer system developers, or for computer operators*. Worse, computer operators are no longer "IT professionals" set apart with a career to manage computers, but now include everyone with access to a PC or mobile device: that is, *anyone* can now modify computer evidence and develop their own documents and spreadsheets. AI systems now create documents that look well-written and can easily be passed off as professional writing, yet they often make numerous, sometimes serious, errors.[3]

While much court evidence passes through spreadsheets, there is no quality control over the processing of data inside spreadsheets. Spreadsheets are an area that is widely recognised to be an unreliable wild west — for instance typos can cause chaos, cells and rows or columns of data can be deleted or corrupted leaving no trail of the changes, whether accidental, deliberate, or caused by bugs. Despite the MoJ's emphasis on software, the majority of errors in spreadsheets and in evidence more generally are caused by humans: spreadsheet users misunderstand details of how spreadsheets work and lose track of details because of spreadsheet complexity. Bugs are not the main problem.

Under an NDA, I interviewed every AI developer in an AI start-up, which was developing software for healthcare infrastructure, with products already in use internationally. The most technical answer I got when I asked them how they developed their systems was that "we tinker." It is worrying that this is a leading company selling systems that appear very persuasive, but it is more worrying that the people who use their AI systems have no way of knowing how unreliable they may be, and when they may behave unreliably. They have no idea what impact their poor design will have, so they give evidence in court that their systems are impressively reliable, but be unable to provide a statistical or other valid argument that the particular evidence they have provided to the court is reliable. The court may also fail to recognise the technical flaws in their evidence. If so, this would be the same error Post Office Horizon prosecutors made: Horizon might make millions of correct transactions, but this was not a valid argument that the particular transactions in the particular evidence presented in court were correct or statistically likely to be correct.

Computers are usually connected to networks and are influenced by the performance and reliability of other computers and data from all around the world. Even if computers are not connected to networks, they were when their software was developed. Thus, computer evidence can be compromised by cyberattacks and by misleading information sourced from anything or anyone *anywhere*.

Routine computer operations such as software upgrades can fail and make arbitrary changes to evidence — the July 2024 CrowdStrike upgrade crashed 8.5 million computers worldwide.[4]

---

[3] See the case reported here: "Norwegian files complaint after ChatGPT falsely said he had murdered his children," Guardian, https://www.theguardian.com/technology/2025/mar/21/norwegian-files-complaint-after-chatgpt-falsely-said-he-had-murdered-his-children, 2025.

[4] BBC, "CrowdStrike IT outage affected 8.5 million Windows devices, Microsoft says," https://www.bbc.com/news/articles/cpe3zgznwjno, 2024.

In short, *modern computers are unreliable*, and in most cases this unreliability is not obvious to users — yet may still have a critical impact on the reliability of evidence.

Manufacturers recognise this unreliability and contrive to avoid liability for problems, typically by forcing users to accept long, complex contracts with a single click that waive their normal rights.[5]

This MoJ call wants to improve the quality of computer evidence, yet everyone has blindspots over computers. The simplest is the widespread acceptance of blanket "end user licence agreements" (EULAs, or warranties) which the manufacturers use to deny to the greatest extent permitted by applicable law any liability for the quality of their systems.

In *R v Cahill, R v Pugh* 14 October 2014 (Crown Court at Cardiff, T20141094 and T20141061) the prosecution evidence relied on a database that was not approved or warranted for clinical use, let alone for evidential use that could put people in prison. The database was later shown to be unreliable, and hence all the prosecution's computer evidence was excluded.[6]

While things are only increasing in complexity, and AI is increasingly used to generate evidence, to compound the situation AI is only the current player in a continuing line of disruptive, cutting-edge digital technology. In only a few years, we have had digital signatures, cloud, mobile devices, dark web, blockchain, AI, bots, quantum computing … and more will come rapidly. While overturning the dangerous Presumption in legislation should be immediate, it will therefore be essential to consider systemic methods to assess the reliability of computer evidence that are future proofed and not locked into particular technologies — we discuss ways to achieve this — and ways to think about this — below.

All my discussion above assumes all parties are essentially well-intentioned people. Of course, in criminal and civil cases this assumption is false: many parties are malicious, and computer evidence provides very many opportunities (beyond those we can cover in the present response to the MoJ) for obfuscation and misdirection.

In addition, a growing problem that must be acknowledged is the possibility of known or unknown malicious third parties, such as cyberhackers (including sophisticated state actors who may be impossible to identify), who undermine the reliability of evidence for reasons independent of specific litigation that may then be seriously affected by corrupt evidence.

(b) How easy or difficult do you believe it is at present for this Presumption to be effectively rebutted?

It is very difficult to rebut the Presumption, because the Presumption is part of the false culture that computers are reliable. Defendants are rarely in a position to identify problems with computer evidence, and are at a huge disadvantage because it is not obvious what questions should be asked to frame rebuttals. Moreover, modern computer systems are very complex and finding problems in huge quantities of data, configurations and software is in many cases technically impractical even if the right questions are telepathically known.

(c) What barriers do you see in effectively rebutting this Presumption?

The Post Office Horizon case shows on a very large scale, across many separate prosecutions and out of court settlements, that it is effectively impossible to rebut the Presumption — with disastrous consequences for many innocent defendants.

Even if the Post Office had disclosed more, the evidence presented to the Post Office Inquiry shows that the documents and knowledge of Horizon were chaotic. Witnesses at the Post Office Group Litigation before (the then) Hon Justice Fraser suggested around five changes were made to Horizon *every working day*.[7] This is likely an underestimate of the rate of change, as software development is normally a continual process, of coding, testing, debugging, etc. Software is a

[5] Disney argued that a person who died after an allergic reaction to food served in a Disney Park had previously agreed to a EULA (for a free trial of a Disney streaming service) excluded liability for the incident (Thimbleby & Thomas, "The Post Office Horizon Scandal: Ensuring nothing like it ever happens again," *Proceedings 33rd Safety-Critical Systems Symposium*, **SCSC-199**:pp361–376, 2025).

[6] Full details and further documents and citations are provided in https://www.harold.thimbleby.net/reeds

[7] Bates v The Post Office Ltd (No 6: Horizon Issues) Rev 1 [2019] EWHC 3408 (QB), [622], https://www.bailii.org/ew/cases/EWHC/QB/2019/3408.html

moving target. Rebuttal is impossible to aim precisely because the prosecution can use complexity and obfuscation to shift the targets.

I want to emphasise again that the problem is not the Presumption *per se*, the problem is not disclosure and rebuttal, the problem is the mess that is the collision of computer technology, incompetent design, and incompetent use. Computer systems are complex and hard to use reliably. Unnoticed errors are easily made, and can make critical evidence unreliable regardless of the quality of the software. As computers are now embedded in all areas of life, it is urgent to address these fundamental problems that undermine the reliability of evidence — and in fact are increasingly causing serious problems that require reliable evidence to sort out.

The MOJ's dilemma is how to do something which improves the use of computer evidence despite the increasing complexity and unreliability of the sector. The MoJ might motivate legislation to improve the reliability of computers and developers and therefore increase the reliability of computer evidence.

2. Are you able to provide examples from other jurisdictions or situations where the reliability of software must be certified?

a) As examples of good practice? b) As examples of things to be aware of?

Military, avionics, air traffic control, and railway signaling are examples of good practice in developing, deploying and using reliable digital systems. Air traffic control and black boxes maintain reliable records of flights to support accident investigations.

I am not sure these examples are good examples of assuring reliable electronic evidence as reliable evidence also requires reliable trained competent operators, and data integrity techniques including digital signatures or equivalent rigorous certification or audit.

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? It would be helpful if your answer could address as many of the below as possible:

a) What procedural safeguards need to be in place to ensure your proposed solution is effective?

I would propose at least the following ideas are seriously considered. All could be achieved, and ideally there would be a timetable for implementing each suggestion; however, even implementing one would be better than none. The proposed solutions call for an alignment with the revision or replacement of the Presumption and necessary improvements in the reliability of computers and computer use themselves. Without strong assurance that computers and computer use are reliable, evidence can never be assumed reliable.

1. Approaches like Reliability of Electronic Evidence Diagrams (REEDs) are used (see https://www.harold.thimbleby.net/reeds). REEDs are diagrams of computer evidence pathways, showing and documenting how evidence is gathered, processed, interacts, and ultimately is presented in court. Beyond understanding evidence in court, REEDs are also best practice for the development and management of computer systems — and provide evidence (if it is the case) that computer systems have been managed in a way to support reliable evidence.
2. If systems used in evidence pathways have EULAs (warranties) that exclude liability for being reliable in a way that could affect the reliability of evidence in a particular case, then the Presumption (or its successor if any) should be automatically rebutted, and the affected evidence excluded. EULAs would need to be checked to ensure that all systems along evidential pathways are reliable or at least adequately reliable for the purposes to which they are put to provide evidence.
3. Computer evidence could be supported by a reliability scoring system, like the widely-used energy ratings of white goods, then computer systems and computer evidence will over time become more reliable. For instance, white goods are now much more energy efficient because consumers are provided with good information to inform better purchases, hence putting market pressure on manufacturers to improve. In fact, the

improvement caused by the clear energy rating system meant the rating system itself has had to be adapted to accommodate the much-improved energy efficiencies! The same would happen with the reliability of computers and the reliability of computer evidence if there was a scoring or rating system available at the point of purchase.

4. As suggested in 1(i), legislation is needed to ensure computer developers, operators, maintenance staff, etc, are certified as competent — analogously to medical or electrical professionals. There should also be a special certification category for digital expert witnesses.
5. Certification in any form (including for lawyers, police, etc) assumes a new, rigorous syllabus to be devised, and the creation of a professional registration body to develop it, as justified in section 3(b) below.
6. Until there is legislation to define and require formal certificates of reliability together with the appropriate certification of the people who provide such certificates, whatever limitations they may have, there seems to be no way to reduce the workload of courts to manageable levels whilst also taking due diligence.

These suggestions as they stand are not exhaustive (see also further complementary *reasoned* ideas in[8,9]), but demonstrate that specific, computationally informed answers are available, and that it may be possible to improve the legislative and procedural framework for safeguards *and* to start to correct the wider culture around computer reliability that currently makes computer evidence so problematic.

b) How might we ensure that any proposed solution is, as far as is reasonable possible, future-proofed?

- One area that needs emphasis is called *computational thinking*. Computational thinking is a teachable skill that is needed — needed to be engaged and available — throughout the legal profession. An important point of computational thinking is recognising when competence in computational thinking is needed.
- Almost all legislation (not just the Presumption) needs some way to become and stay digitally literate since computers are changing and revolutionising all areas of modern life (gambling, contracts, bills and payments, healthcare, education, supply chains, to name a few of the more obvious examples). Some areas of modern life (such as social media) did not even exist a few years ago; their pervasive legal and regulatory influence, such as their impact on child safeguarding, had not even been anticipated in science fiction.
- Courts should only accept evidence if it (including the system management and evidence pathways that generated it) has been audited and certified as reliable. To do so would drive both a certification market and increasingly more reliable computer systems, as suggested above. Currently, however there is no technically adequate professional framework enforced to support certifying computers evidence.
- Universities should be urged to develop advanced and technically-relevant qualifications in computer reliability. Indeed, the qualifications of software engineers needs improving, including making certification to practice (as in other critical industries) essential. Professional organisations should develop CPD (continual professional development) programmes and certificates analogous to existing regulation of professionals certified to operate in areas such as gas or electrical reliability.

Education for legal professionals, expert witnesses and other professionals who prepare and handle evidence needs expanding to include digital awareness and competencies.

[8] P Marshall, J Christie, PB Ladkin, B Littlewood, S Mason, M Newby, J Rogers, H Thimbleby & M Thomas, "Recommendations for the probity of computer evidence," *Digital Evidence and Electronic Signature Law Review*, **18**:18–26, 2021. DOI 10.14296/deeslr.v18i0.5240

[9] S Mason & D Seng, *Electronic Evidence and Electronic Signatures*, 5th ed (see especially Chapter 5, The presumption that computers are 'reliable'). Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2021. Open sourcehttps://uolpress.co.uk/book/electronic-evidence-and-electronic-signatures

- A professional body should be established, in particular to be charged to stay abreast of technical innovation. Moreover, it needs to be a *new* body with specific duties to do this, as none of the existing, traditional professional bodies have realised that computers are undermining the reliability of the areas of expertise (e.g., medicine) they are supposed to regulate. For example, the British Computer Society and the Institution of Engineering and Technology provide very easy routes to Chartered Engineer status that can be contrasted with the Institution of Engineering Technology's rigorous approach to certifying electricians. The problem establishing a new professional body avoids is the temptation to merely extend (as BCS and IET did) their existing membership into a default Chartered Engineer status with no specific qualifications required.

The Medical Act 1858, mentioned above in section 1a(i), established the General Medical Council for analogous reasons — to escape the inertia of existing medical clubs — and to set higher standards for medical qualifications. Arguably, then, a "General Digital Council" should be established as part of the MoJ's agenda to bring the computer evidence area up to date *and to keep it up to date* in exactly the same way the GMC has evolved and updated its remit since its founding.

This organisation should also develop a syllabus and exams, with regular planned revisions to remain up to date, to train judges, lawyers, police and others who interpret or who are responsible for reliable evidence.

c) How might we ensure that any proposed solution is operationally practical?

Legislation must avoid so far as possible what is called *implementation bias*. Mentioning any specific forms of implementation (e.g., "text message" or "AI", whatever) ensures the legislation is *not* future-proofed.

I suggest that Reliability of Electronic Evidence Diagrams (REEDs, https://www.harold.thimbleby.net/reeds) are a practical and easily understood way to facilitate thoroughly exploring electronic evidence and identifying problems and lacunae, while at the same time avoiding implementation bias. REEDs effectively make the examination of evidence become much less technical for legal professionals and the public – including defendants and juries.

d) If your proposed solution requires the use of expert witnesses (either jointly or singly instructed), what expertise and qualifications would that person require? To your knowledge are there sufficient such people at present?

There are not sufficient numbers of competent people available at present, and there are not adequate and adequately rigorous qualifications available to set standards for training or qualifications. Without a suitable educational framework, it is impossible to recognise qualified and competent people. This problem creates a vicious cycle. For instance, there are very few rigorously trained software engineers, so the democratic majority view on software qualifications is that qualifications should continue to be weak.

It is worth emphasising that REEDs give a non-technical way of exploring evidence and understanding evidence pathways, and hence lower the levels of computer expertise needed. REEDs also help make any incompetence in generating and preparing evidence more visible.

4. In your opinion, how should 'computer evidence' for these purposes be best defined?

a) Do you agree that evidence generated by software, as set out above, should be in scope, and that evidence which is merely captured / recorded by a device should be out of scope? Please provide a rationale for your answer.

Once a computer is involved, and it is hard to avoid them, there is no such thing as evidence that is "merely" captured or recorded by a device. Programmable computers, including common applications like spreadsheets and word processors — which are routinely used in preparing evidence — can do anything to recorded evidence; they can also suffer cyberattack.

Three examples will suffice:

- Infusion pumps are devices that deliver drugs automatically to patients. H Thimbleby's *Fix IT* (Oxford University Press, 2021) gives many examples of computer unreliability in healthcare. One detailed example is a BBraun infusion pump that has bugs that cause nurse errors in setting drug doses, and also records them incorrectly in its data logging — so if a BBraun device logs are used in evidence, they may record errors caused by the bugs and not by nurses.
- Many complex decisions are programmed on Excel spreadsheets by administrators or non-technical police or CPS staff, *and things go wrong*.
- The present MoJ call for evidence wants to exclude computer evidence such as text messages from any revision of the Presumption yet, while this is understandable, there is no technical reason to think that text messages are immune to the reliability problems of all other digital technologies. For example, if the police seize text message data, how will they ensure and be able to prove they have ensured that the data they present as evidence is exactly the data they thought they seized?

There has to be an auditable evidence pathway resulting in a secure digitally signed document, and there needs to be ways to assure the evidence has not been tampered with against the signature(s). There should at least be a legal requirement for digital signatures, and a reliable, secure repository for cases where digitally signed documents can be archived and shared amongst securely identified parties.

i) Can you provide specific examples of the type of evidence you believe should be in scope?

It is hard to think of any type of evidence that should not be in scope.

Even evidence presented in person by people will likely have been influenced by or had its direct origins in computer systems. The Cameron case is a recent example where the Appeal Court argued that the case was not a "Horizon case" even though the human evidence used by the prosecution had been obtained entirely from financial evidence taken from Horizon computer output.[10]

Another example is the Home Office claimed someone, known as AH, returning to the UK was subject to a deportation order. The Home Office claimed AH had already been deported and had an extensive criminal record. Initially the Home Office accepted AH had been confused with another person, but then despite evidence of their errors, the Home Office sent AH a letter asserting he was a deportee using a false identity. After a judicial review, the Home Office conceded that officials had "mixed up files."[11] This is an example where computer evidence is apparently reliable, but the authorities have unwittingly used the *wrong* computer evidence. Ironically, the Home Office knew they had problems with their immigration database, and had initiated changes to improve its reliability which then erroneously merged identities. This is yet another example of an organisation — in this case, a substantial state organisation — using incompetent developers and processes to undermine the reliability of what it uses as computer evidence.

Furthermore, many products that are not normally thought of as "computers" now contain embedded computers that can make arbitrary changes to data or logs that may be used in evidence. Modern cars, for instance, are controlled by many computers, including supporting driverless operation, so after accidents manufacturers will want to argue that their complex systems did not cause the accidents. There are many examples of manufacturers who did not cooperate with the expert witnesses who needed to examine the evidence.[12] Cars even routinely delete relevant evidence (e.g., of accelerator/brake failure).[11]

---

[10] P. Ladkin, S. Mason & H Thimbleby, "Misunderstanding Digital Computer Technology in Court: A Commentary on a Case Involving the Post Office Horizon System," *Digital Evidence and Electronic Signature Law Review*, **21**, 2024. https://journals.sas.ac.uk/deeslr/article/view/5776/5406

[11] C. Baksi & J Ames, "Dutch resident barred from UK for seven months after ID mix-up," *The Times*, p20, 2 April 2025.

[12] M. Barr, *BOOKOUT V. TOYOTA, Camry L4 Software Analysis*, 2005. https://homepage.cs.uiowa.edu/~tinelli/classes/181/Fall14/Papers/Barr13.pdf

Regardless of concerns about the competence of the developers of car systems, there is no regulation to require controlled documentation of the quality control processes that may be used, and there is no certification available that a court could accept at face value without engaging highly skilled technical expertise to interpret it — which the car manufacturers would resist because of commercial confidentiality reasons. Furthermore, the car manufacturers and software developers could be headquartered outside UK jurisdiction. Analogous issues face *all* industries and hence *all* computer evidence. There are therefore *in principle* no areas that should be out of scope.

I believe the MoJ wants to define some areas as out of scope because it does not want to face the apparently daunting scale of problems that could arise by admitting that in principle really nothing should be out of scope. For example, if text messages are in scope there may be many text messages for a court to consider and this would be burdensome. However, the technical difficulty is not the number of text messages, but the various ways in which text messages can be corrupted or edited after the fact, and that is exactly what a court should examine. A court must establish that the evidence it is using is the right evidence and is reliable for the purposes of the case. Again, REEDs provide a way of helping a court understand the evidential pathways and the potential strengths and weakness of the evidence.

In many cases, computers themselves (provided they are appropriately designed and certified, etc.) can provide tools, such as machine learning and data visualization, to help rigorously analyse evidence, hence turning the apparent overwhelming quantity of computer evidence into something entirely manageable.

ii) Can you provide specific examples of the type of evidence you believe should be out of scope?

An example of when a type of evidence could be out of scope is when a competent person, such as a registered pathologist, can vouch for the quality of their own evidence, and can be cross examined on the computer presentation or summary of that evidence. (For instance, using evidence generated by using a digital microscope.) The competent person can then attest the reliability of documents and pathology images, etc, that fall within their expertise.

5. Are there any other factors which you believe are important for us to consider?

Longer term solutions will have to improve "digital maturity" and competently using computational thinking to manage, examine and audit all evidence pathways, urgently in the CPS and police. This will require education, and definition of certified persons, as in other critical industries.

Longer term solutions will have to embed routine auditing of the use of computer evidence in cases (randomly sampled to keep the audit load reasonable), and ways for the learning from such auditing to be summarised and adopted.

Digital technologies are accelerating ahead of any professionals to keep up — even including researchers in digital technologies.

The MoJ at least, and the Attorney General's Office, and the Department for Science, Innovation & Technology should establish a new department to keep abreast of and provide legal advice on the issues outlined in this response to the MoJ call for evidence.

Any such new department will need to have careful recruitment strategies to avoid perpetuating the current technically immature digital culture. Proactive links with university departments of computer science in the UK and internationally are to be strongly recommended for this is an international legal problem not limited to the UK.

Summary

This submission's main proposals are covered in section 3, primarily in 3(a)1–6. While rigorous, these and other ideas expressed throughout this document are not easy proposals. It might be tempting, then, to quickly dismiss them as "the best is the enemy of the good," but if the MoJ does not at least aim for the best, it will never get close to useful improvement.

A core proposal is to use REEDs, Reliability of Electronic Evidence Diagrams, as explained fully in https://www.harold.thimbleby.net/reeds REEDs are essentially a non-technical approach to support the understanding of electronic evidence. They can be used in pre-proceeding discussions, and can also be used in preparing and critiquing evidence, and in documenting the design, maintenance and use of computer systems.

This submission to the MoJ is abridged from a more substantial document/presentation that is available from the author; please email me at harold@thimbleby.net

As Voyager 1 shows, we can have reliable computer evidence if we have competent developers, competent system managers *and the will — backed by legislation— to build and operate reliable computer systems that assure reliable evidence*.