Submission to Call for Evidence on the role of computer evidence in the criminal justice system

14 April 2025

1. **Graham Smith** is a solicitor in private practice with Bird & Bird LLP in London. He joined Bird & Bird in 1983 as an associate, continuing as a partner from 1985 to 2019 when he assumed his current Of Counsel position. His experience ranges from intellectual property and IT litigation to advising on technology-related subjects such as software copyright, interception of communications, investigatory powers and lawful access, electronic signatures, and online intermediary liability and regulation.

2. He is the main author and editor of the textbook *Internet Law and Regulation* (Sweet and Maxwell, 5th ed 2019). He gave evidence in 1997 to the House of Lords Science and Technology Committee Inquiry on Digital Images as Evidence, and in December 2015 to the Joint Scrutiny Committee on the draft Investigatory Powers Bill. He was a member of the external Advisory Panel for the Law Commission Report on Electronic Execution of Documents (LawCom No. 386, 2019). He is the author of the Cyberleagle blog.

3. This submission is made in Mr Smith's personal capacity and represents his personal views. It is not attributable to his employer, nor to any of its clients.

A. PRELIMINARY

4. I should make clear at the outset that I do not profess experience in or any particular insight into the operation of the criminal justice system. My litigation experience has been in the civil courts. As a technology lawyer, however, I have from time to time considered the subject of computer evidence. Specifically, this included a 1994 article in *Computer Law and Security Review* ('When is a computer not a computer?'), surveying some of the then current caselaw on computer evidence, including cases on Section 69 PACE 1984. *Internet Law and Regulation* contains a more general section on evidence.

5. I shall therefore largely confine my submission to examining the common law evidential presumption in the light of the reported caselaw and putting the presumption in context, identifying some lessons that can be learned from the caselaw that developed around the Section 69 PACE regime, and identifying some broader questions that it seems to me have to be considered alongside the formal evidential presumption.

B. THE CHALLENGE

6. This Call for Evidence[1] has been prompted, following the Horizon debacle, by calls[2] for the common law evidential presumption of reliability as applied to computer systems to be revisited.

7. The 1995 and 1997 provisional and final recommendations of the Law Commission to abolish S.69 PACE and revive[3] the common law presumption have been criticised on multiple grounds, including (a) an assumption that errors in computer systems would readily be evident to their users and operators from the system's output, or would result from input errors (b) analogising complex IT systems to breathalyser machines and (c) underestimating the difficulty faced by a defendant in rebutting the presumption in the absence of access to information about the workings of the computer system in question[4]

8. The challenge has always been, and remains, to fashion an evidential regime in criminal proceedings that is both principled and workable; that enables justice to be done and also prevents injustice. In my view, for reasons that I shall explain, that requires a wider perspective than focusing solely on the formal evidential presumption of reliability. That would not take into account broader and deeper manifestations of an informal tendency

---

[1] The Call for Evidence is restricted to criminal proceedings. Civil proceedings, thanks to the different standard of proof, different procedures, different disclosure rules, more flexible rules about hearsay, and trial by judge rather than jury, are significantly different. I would endorse their exclusion from this Call for Evidence. It is noteworthy that it was in civil proceedings that the Horizon problems were successfully brought to light.

[2] The Call for Evidence was specifically in response to an amendment proposed by Baroness Kidron et al to the current Data (Use and Access) Bill. The proposed amendment was framed as a set of conditions for reliance on (or, in the amendment's earlier version at Committee stage, for admissibility of) computer produced or derived evidence. I would comment that as drafted it could raise the question of whether it was intended to be an independent self-standing gateway to admissibility or reliance for any kind of computer evidence, or a condition that would have to be satisfied <u>in addition</u> to other potentially applicable conditions e.g. as to hearsay evidence. As I discuss in para 109, the same question arose with S.69 PACE. On this point the final version of S.69 changed compared with the original Criminal Law Revision Committee proposal in 1972, which was framed similarly to the Baroness Kidron et al amendment.

[3] S.69 PACE 1984 did not abolish the common law presumption as such. At first, some authorities suggested that the presumption could be deployed to satisfy the requirements of S.69(1) (*R v Blackburn, R v Wade* (The Times, 1 December 1992) and cases cited therein). The House of Lords held otherwise in *R v Shephard* [1993] A.C. 380 at 384E. The understanding of what was within the scope of S.69 also changed in other ways. Initially it was thought that S.69 applied only to hearsay statements in documents produced by computer (*R v Minors*, *R v Harper* [1989] 1 W.L.R. 441 (C.A.), *R v Spiby* (1990) 91 Cr.App.R. 186 (C.A.). That persisted until *R v Shephard* (at 386C). Following the repeal of S.69 the common law presumption could be relied upon once again.

[4] Numerous papers have been written about the Law Commission's recommendations, including: P. Ladkin et al: *The Law Commission presumption concerning the dependability of computer evidence* DEESLR, 17 (2020) 1; P. Marshall et al: *Recommendations for the probity of computer evidence* DEESLR, 18 (2021) 18; N. Bohm et al: *The legal rule that computers are presumed to be operating correctly – unforeseen and unjust consequences* Bentham's Gaze (UCL blog) 30 June 2022; J. Christie: *The Law Commission and section 69 of the Police and Criminal Evidence Act 1984* DEESLR, 20 (2023) 62; S. Mason: *The presumption that computers are reliable* Counsel Magazine, 10 July 2024; S. Mason: *The UK Post Office Horizon IT scandal: Part 2: the legal issues* C.T.L.R. 2024 30(4). For some contemporaneous commentary, see V. Collins: *Computerised Evidence: Finding the Right Approach* Nottingham Law Journal Vol 3 1994 11-33; A. Hoey: *Analysis of the Police and Criminal Evidence Act s.69 – Computer Generated Evidence* [1996] 1 Web JCLI and K. Quinn *Computer evidence in criminal proceedings: Farewell to the ill-fated s.69 of the Police and Criminal Act 1984* The International Journal of Evidence and Proof, Vol 5 Issue 3, July 2001 174-187.

to assume that the computer is right unless shown otherwise, and which is equally (if not more so) capable of leading to injustice.

C. TECHNOLOGICAL PROGRESS

9. It is a trite observation that the Law Commission's 1995 and 1997 recommendations were made at a time when computer systems were nothing like as pervasive as they are in the present day world of smartphones and the ubiquitous internet. Nevertheless, it would be a mistake to think that the current issues surrounding computer evidence were not recognised, as a matter of kind if not degree, by at least the 1980s.

10. The competing considerations were well articulated in 1988 by Steyn J. (as he then was) in *R v Minors, R v Harper* [1989] 2 All ER 208 (C.A.):

> "The law of evidence must be adapted to the realities of contemporary business practice. Mainframe computers, minicomputers and microcomputers play a pervasive a role in our society. Often the only record of a transaction, which nobody can be expected to remember, will be in the memory of a computer. The versatility, power and frequency of use of computers will increase. If computer output cannot relatively readily be used as evidence in criminal cases, much crime (and notably offences involving dishonesty) will in practice be immune from prosecution. On the other hand, computers are not infallible. They do occasionally malfunction. Software systems often have 'bugs'. Unauthorised alteration of information stored on a computer is possible. The phenomenon of a 'virus' attacking computer systems is also well established. Realistically, therefore, computers must be regarded as imperfect devices."

11. That was 7 years after the launch of the IBM PC and 4 years after the Apple Macintosh. With the addition of mobile and internet-enabled devices to the inventory, and recognition that formerly analogue mechanical devices tend now to be digital[5], that passage could hardly be bettered today.

12. As a matter of degree (some might say kind) the biggest difference is probably the extent to which documents are now generated, stored and transmitted by means of networked third party devices and systems (cloud computers, the internet and social media). Obtaining evidence of the design and functioning of some third party systems could be especially challenging.[6]

13. The pervasiveness of computerised systems and networks, coupled with migration from analogue to digital devices, does mean however that the consequences of getting the criminal evidentiary regime wrong are much more far-reaching than they were in 1988:

---

[5] For an example of such a transition (car braking systems) and its possible implications for judicial notice (and, implicitly, evidential presumptions), see Stephen Mason and Daniel Seng *Electronic Evidence and Electronic Signatures* (U. Lon. Press, 5th edition) paras 5.18 and 5.19.

[6] As to networking, cf. Law Commission Consultation Paper No.138 1995, para 14.14; Report, para 13.8. For a recent fraud prosecution that depended on evidence obtained from a third party system, in which admissibility was unsuccessfully challenged, see *R v AEB* [2024] EWCA Crim 1320. In *O'Shea v R* [2010] EWCA Crim 2879 evidence of credit card details was obtained from the database of a third party website (previously closed down by US authorities) which the defendant was alleged to have accessed in order to obtain indecent images of children.

whether in the potential for miscarriages of justice experienced by defendants, in prosecutors failing to obtain the convictions that justice would expect, or both.

14. It should not be forgotten that computer evidence adduced by the prosecution may include evidence originating from the defendant's own systems, for instance where computers and devices belonging to defendants have been seized and analysed by the prosecution. Nor should it be forgotten that defendants themselves may seek to adduce computer evidence[7].

15. Proposals for change have focused on, or at least been prompted by, avoiding a repeat of Horizon. However, as the Call for Evidence recognises, a regime for dealing with evidence derived from computer systems has to be suitable for all manner of different kinds of information, systems and circumstances. Barely any document will now not at some point in its history have been touched by a computer. A regime for computer evidence is, by and large, now synonymous with a regime for documentary evidence[8].

D. SCOPE OF THE CALL FOR EVIDENCE

16. Although the specific questions annexed to the Call for Evidence are focused on the suitability of the evidential presumption that a computer is operating properly, the Introduction is cast more broadly: the way in which evidence produced by software (which I take to include computers generally) is handled in criminal proceedings. The role of disclosure in criminal proceedings is also noted.

17. That broader approach is, in my view, strongly preferable to focusing on the evidential presumption in isolation. As I will develop, it appears to me that the formal presumption cannot sensibly be divorced from informal assumptions about reliability of computers that may influence other aspects of criminal procedure, such as disclosure and the fundamental notion of proof beyond reasonable doubt.

18. Nor is it clear to me (speaking with the limited knowledge of a non-criminal practitioner) how much of a role the presumption itself actually plays in the day-to-day conduct of criminal proceedings, outside the well-trodden areas of breathalysers, radar speed guns and other purpose-designed law enforcement equipment[9]. Be that as it may, it seems to

---

[7] One example would be a defendant who sought to rely on a video that they had taken on their own mobile phone.

[8] The Law Commission 1995 consultation paper noted at para 14.24 that 'computer records are usually business records'. That may have changed. For instance, video evidence adduced in the criminal courts court now includes dashcam footage https://yorkshiretimes.co.uk/article/The-Growing-Role-Of-Dashcam-Footage.

[9] As regards Horizon, the Explanatory Note to the Baroness Kidron et al Data (Access and Use) Bill amendment states that the presumption "contributed to miscarriages of justice including the Horizon Scandal". A blogpost by journalist Nick Wallis in December 2024 said: "Although the "mechanical instruments" presumption has never, to the best of my knowledge, been quoted in any civil or criminal proceedings involving a Subpostmaster, it has been said to effectively reverse the burden of proof on anyone who might be convicted using digital evidence." (www.postofficescandal.uk/post/proposed-amendment-to-legal-assumption-about-the-reliability-of-computers/). The submission of the Criminal Cases Review Commission to the Post Office Horizon IT Inquiry (28 January 2021) makes observations on the presumption at para 74. The most publicly documented criminal prosecution known to have gone to trial (Seema Misra) made no express reference to the evidential presumption, either in prosecution submissions or in the judge's summing-up. Stephen Mason has suggested that

me that the application of the presumption to general purpose computing systems is the main focus of the current debate.

19. The evidential presumption of regularity, properly so called, has a specific legal function in criminal proceedings: to fill what would otherwise be a gap in the admissible[10] evidence at trial necessary to prove the offence. That is different from an informal tendency to ignore or underestimate the extent to which software is prone to error, which may manifest itself in a variety of different ways, any of which are capable of resulting in injustice.

20. For instance the prosecution's approach to disclosure requests might be influenced by an informal attitude, or perception, that the computer is right unless shown otherwise; and therefore that it is for defendants to justify requests for disclosure by demonstrating specific grounds to doubt the reliability of the system.

21. That sort of approach was deprecated by the Court of Appeal as, in effect, seeking to reverse the burden of proof[11]; but neither that approach itself nor an underlying assumption about reliability of computers is quite the same thing as relying on the formal evidential presumption of reliability to fill a gap in evidence at trial or on appeal[12]. However, the outcome of a defendant's application for disclosure may be affected by whether the presumption of reliability is in fact being relied on at trial.[13]

22. These distinctions may seem somewhat legalistic, but I would suggest are important given the specific focus of the Call for Evidence on the presumption of reliability, properly so called.

---

the prosecution submissions implicitly relied upon it (S. Mason: *The UK Post Office Horizon IT scandal: Part 2: the legal issues* C.T.L.R. 2024 30(4)).

[10] Rules of evidence in criminal proceedings place much more emphasis on admissibility than do civil rules, due to considerations of what evidence is appropriate to be put before a jury.

[11] *Hamilton & Ors v Post Office Ltd* [2021] EWCA Crim 577, [137].

[12] Peter Ladkin ('Disclosure and the Common Law Presumption that Computers are Reliable') notes that the formal presumption and disclosure obligations are separate issues and should not be elided. That, however, is not a reason to consider only the formal presumption.

[13] The defendant may apply under S.8 Criminal Procedure and Investigations Act 1996 if they have served a defence statement and have reasonable cause to believe that the prosecution has material that satisfies the disclosure test. In *Rothon v DPP* [2005] EWHC 2986 (QB) (an Intoximeter case) the justices held the hearing of the case in three parts, the second part being a disclosure application which they refused. On an appeal from conviction by way of case stated Crane J. held that if the justices were in fact applying the presumption of reliability they would have been entitled to refuse disclosure. However, they heard evidence from an expert on behalf of the prosecution. Once they had done that, the position changed and they should have acceded to an application for disclosure. Conversely, in *DPP v Manchester and Salford Magistrates Court* [2017] EWHC 3719 the Divisional Court cautioned that unless disclosure applications in cases involving the type of breathalyser in issue were focused in the way identified by the court, then "this extensive disclosure would have to be given in every case in which a defendant alleged that his alcohol consumption had been too low to sustain a positive reading, and in effect proof of reliability would always be required and the presumption of accuracy would be displaced". A mutual relationship between application of the reliability presumption and the calling of expert evidence can also be seen in the remarks of Senior District Judge Riddle in *CPS v Cipriani* at 6c, annexed to *R (Hassani) v West London Magistrate's Court* [2017] EWHC 1270 (Admin).

23. To summarise, the **formal evidential presumption** should (I suggest) be distinguished from an **informal assumption or perception that computer evidence is generally reliable**. The latter may manifest itself in a variety of different contexts, of which the formal evidential presumption is only one. The evidential presumption itself is not necessarily either the beginning or the end of the matter. The scope of the review should be broad enough to cover all possible manifestations.

E. OBSERVATIONS ON THE EVIDENTIAL PRESUMPTION OF RELIABILITY

24. As described by the Law Commission in its 1995 and 1997 recommendations (quoting *Phipson on Evidence*), the presumption of regularity is:

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

25. The Law Commission also said:

> "Without section 69, a common law presumption comes into play:..." (1997 Report, para 13.13)

And:

> "We are concerned about smoke-screens being raised by cross-examination which focuses in general terms on the fallibility of computers rather than on the reliability of the particular evidence. The absence of a presumption that the computer is working means that it is relatively easy to raise such a smoke-screen." (1995 Consultation Paper, para 14.20)

And:

> "If there were no pre-condition for the admission of computer records, the parties would be able to rely on the presumption of regularity. ... The principle has been applied to such devices as speedometers, traffic lights and Intoximeters; we see no reason why it should not apply to computers." (1995 Consultation Paper, para 14.28, citing *Castle v Cross* for the proposition that there is no requirement that the instrument in question should be of a kind which is commonly known to be in working order more often than not.)

And:

> "We are satisfied that the presumption of proper functioning would apply to computers, thus throwing an evidential burden on to the opposing party" (1997 Report 13.23)

26. These statements appear to assume that the presumption would apply automatically to all kinds and examples of computers in all cases in which there was no evidence to the contrary.

27. That might be thought to place more weight on *Castle v Cross* than it can readily bear[14]. Specifically:

    - *Castle v Cross* was a prosecution appeal from a successful submission of no case to answer at the end of the prosecution's case on a charge of failing to provide a specimen of breath.
    - It concerned a printout from one device (an Intoximeter) that included some computer controls.
    - The printout recorded 'One no sample'.
    - At least arguably, the *ratio* of the case was that the printout was admissible as real evidence and was not excluded as hearsay.
    - The court also held that the police sergeant ought to have been allowed to give direct evidence of what he had observed (Kennedy J described that as the central issue).
    - As to the presumption of reliability, Stephen Brown LJ (with whom Kennedy J. agreed) said: "It has to be assumed, certainly for the purposes of the submission of no case to answer, that it was in proper working order and that the proper procedure was followed." That statement is perhaps somewhat equivocal as to whether the presumption would necessarily have been applied at the conclusion of the trial.
    - In any case, that statement was made in the context that the case stated by the justices "does not record any finding *or indeed submission* that the Intoximeter was in any way defective" (emphasis added).
    - Accordingly: "The question of computer error does not enter into the ambit of this appeal."

28. So, really, does *Castle v Cross* amount to anything more than a finding that the presumption is <u>capable</u> of applying to a computer device? Of course, the presumption has since come to be routinely relied upon for breathalyser and other purpose-designed road traffic law enforcement devices, not least so that the time of the courts is not taken up with prosecution experts having to fend off scattergun assaults on general reliability of well-established equipment. However, it is a considerable leap to treat *Castle v Cross* as authority for the proposition that the presumption would automatically apply to all kinds of computer devices.

29. It is perhaps also noteworthy that, as the court emphasised, there was no recorded suggestion by the defence that the printout 'One no sample' was inaccurate. The appeal was, in effect, on a pure technicality. Indeed, on the facts as reported it might be thought that instead of applying the presumption the justices could adopt the position suggested in *Scott v Baker* (1968) (Div Ct) 1 QB 659 at 673: that if issue has not been taken that could amount to an admission by the defence.

---

[14] Four years earlier, in its 1991 Consultation Paper No. 117 on the Hearsay Rule in Civil Proceedings, the Law Commission was more circumspect in its comments on *Castle v Cross*, which it said concerned "a mechanical intoximeter device which was partly computer controlled": "This presumption in favour of regular operation which applies to mechanical devices may, eventually, be extended to computer driven operations as the two types of operations come to regarded in the same way." (para 3.67).

30. There appears to be a similar theme in subsequent reported criminal appeals. In those that I have found (I readily stand to be corrected if there are others) that involve general purpose computers[15] and apply *Castle v Cross*, there was no assertion that the computer output sought to be rendered admissible was inaccurate.

31. The cases that I have been able to find are: *R v Spiby* (1990) (CA) (hotel automated telephone call records) - would have been justified in applying the presumption, but unnecessary since there was positive evidence; *R v Blackburn, R v Wade* (1992) (CA) (invoices) - presumption of reliability applied so as to satisfy the evidential requirements of S. 69(1) PACE 1984[16]; *PPS v McGowan* (2008) (NICA) (till roll seized from defendant's cash register adduced as evidence of after-hours alcohol sale) - "particularly strong presumption in the case of equipment within the control of the defendant who alone would know if there was evidence of incorrect operation or incorrect setting".

32. There are other questions about the application of the presumption.

33. First, can the ability of the prosecution to rely on the presumption be stymied by a mere challenge (in effect, putting the prosecution to proof)? According to the authoritative textbook formulations the answer is no: there has to be some evidence to rebut the evidential presumption. However, that conclusion had to overcome *Scott v Baker*, in which a bare challenge supported by no evidence was sufficient to prevent reliance on a presumption that a breathalyser was duly approved by the Secretary of State.

34. The explanation for that decision given by the Divisional Court in *Campbell v Wallsend Slipway and Engineering Co Ltd* [1977] (per Lord Widgery C.J. and Eveleigh J.) was that the bare challenge did not in fact rebut the evidential presumption. Instead, the court in *Scott v Baker* had decided that the "situation of that case did not justify applying that presumption" in the first place.

35. The textbook formulations thus describe[17] the position where the presumption applies, but *Campbell v Wallsend* adds force to the proposition that application of the presumption of reliability is not automatic. Particularly in a criminal case, the court appears able to determine that it should not be applied[18].

---

[15] General purpose software and computer systems can be contrasted with breathalysers, radar guns and other devices designed for law enforcement and operated by police officers (while recognising that the presumption has also been applied to mechanical devices such as speedometers). For such devices the presumption of reliability is certainly applied where the defence disputes the accuracy of the measurement.

[16] The subsequent House of Lords decision in *R v Shephard* held that the presumption could not be used to satisfy S.69.

[17] With the possible qualification that the Court of Appeal in *R v Shephard* (1991) 93 Cr. App. R. at [143] articulated the basis for shifting the evidential burden back to the prosecution as "evidence to the contrary, or some reason to doubt the proper functioning of the computer". Although the House of Lords subsequently held that the presumption could not be relied upon in order to satisfy S.69 PACE 1984, it did not comment on this formulation of the presumption. 'Evidence to the contrary' is not necessarily evidence obtained independently by the defence. It could consist of material disclosed by the prosecution in fulfilment of its disclosure obligations.

[18] And see *Rothon v DPP* and *CPS v Cipriani* (fn 13 above).

36. The court in *Campbell v Wallsend* also drew a distinction between novel and well-established situations:

> "…the situation in which the presumption could be invoked had not before come before the courts. Presumptions of law have developed over the years after the courts have seen the cogency of certain inferential evidence from established facts until a point where those established facts can be relied upon to give rise to an inference. No such stage of development had been reached in *Scott v Baker*."

37. This passage is reminiscent of the qualification to the presumption of mechanical reliability stated in *Cross on Evidence* (5th edition) , that "the instrument must be one of a kind as to which it is common knowledge that they are more often than not in working order". Stephen Brown LJ in *Castle v Cross* preferred the formulation in *Phipson on Evidence*, which omitted that qualification.

38. However, that does not appear to negate the general principle of incremental development (my terminology) of presumptions[19] expressed in *Campbell* (which case was not referred to in *Castle v Cross*). *Cross & Tapper on Evidence* (as it now is) continues to maintain that some such qualification is necessary, citing Lord Griffiths in *Cracknell v Willis* [1988] 1 A.C. 450:

> '…that "trial by machine" is an entirely novel concept and should be introduced with a degree of caution'.[20]

39. Incremental development of presumptions is a far cry from applying a general presumption of reliability automatically to every kind of computing device.

40. Another potential fly in the ointment of the reliability presumption is the statement in some authorities that the parent *omnia praesumuntur* presumption should not be applied to criminal prosecutions where the fact sought to be proved is central to the offence. Thus the Privy Council in *Dillon v The Queen* stated:

> "It is well established that the courts will not presume the existence of facts that are central to an offence" *Dillon v The Queen* (1982) (PC)

41. *Dillon* held that the lawfulness of custody was not to be presumed in a prosecution for the offence of negligently permitting a prisoner's escape from lawful custody. It cited, inter alia, *Scott v Baker*, in which Stephen Brown LJ said:

> "I think for myself that one ought to take very great care in a criminal case as to the length one goes in applying that presumption. … Bearing in mind that this is a criminal case, it seems to me that it would be going much too far to press the presumption of *omnia praesumuntur* to the length of saying that there was a prima facie case here that the device used was of a type approved by the Secretary of State."

---

[19] A general presumption that a device of a particular kind is reliable, from which it can be inferred (with any necessary additional evidence as to e.g. calibration) that the particular device was operating properly at the relevant time may be difficult to distinguish from taking judicial notice of such general reliability. See Stephen Mason and Daniel Seng *Electronic Evidence and Electronic Signatures* (U. Lon. Press, 5th edition), para 5.11 et seq.

[20] *Cross and Tapper on Evidence* (R. Munday, OUP, 13 ed. (2018)) p.38.

42. Lord Widgery C.J. in *Campbell v Wallsend* also noted, when distinguishing *Scott v Baker*, that "the matter to be proved was an essential part of the offence itself", whereas the matter in *Campbell* was procedural.

43. The Law Commission 1997 Report observed that if *Dillon* were to be taken literally the presumption could not have been applied in the breathalyser cases (in which the *Dillon* argument did not appear to have been raised). It also suggested that this qualification might apply only to the official action presumption, which was now separate from the mechanical instruments presumption.

44. If nothing else, the decision in *Dillon* may provide a further basis on which to justify a court declining to apply the presumption of reliability according to the circumstances of the case.

45. The Law Commission took the view that a presumption of mechanical reliability is separate from the official action presumption. Whether or not it is, strictly speaking, a separate legal category, in terms of its factual nature the presumption of mechanical reliability is certainly quite a different animal from a presumption that (for instance) someone carrying out a public office has been duly appointed.

46. The public office question is susceptible of a binary, yes/no answer. Analogue mechanical reliability is potentially more graduated, but still capable of relatively clear answers. Reliability of computer systems and software is a far more elusive and nuanced notion, involving malfunctions that can be unpredictable in occurrence and consequences, latent, intermittent and discontinuous[21]. One might think, therefore, (assuming that the application of the reliability presumption is indeed not automatic) that it would be more open to a court in the case of digital systems to decide whether or not in a particular case it is justifiable to apply an evidential presumption of reliability to the particular kind of system.

47. Overall, therefore, notwithstanding the Law Commission's apparent expectation in 1995 and 1997 that the presumption would apply as a matter of course, I would suggest that the caselaw provides **grounds to believe that the presumption would not necessarily be applied routinely to all kinds of computing devices in criminal cases**. That said, there is **little clarity or certainty about when it would and would not be applied to general purpose computing systems**.

The presumption of reliability and proof beyond reasonable doubt

48. The legal burden of proof is conceptually different from an evidential presumption. An evidential presumption does not alter the legal burden of proof - it is a means by which the legal burden of proof may, in some limited circumstances, be discharged without adducing actual evidence.

49. To the extent that the courts have expressed caution about applying the presumption of regularity in criminal cases, the reason is self-evident: the burden on the prosecution is

[21] See Professor Peter Sommer's Response to this Call for Evidence at paras 30 to 34.

to prove its case beyond reasonable doubt, yet the presumption relieves the prosecution of adducing any evidence at all to prove the fact in question[22].

50. 'Beyond reasonable doubt' is not, of course, 'beyond all theoretical doubt'. The deeper question, then, is what doubt may a jury (or other trier of fact) reasonably (as opposed to theoretically or fancifully) harbour about the reliability of computer evidence put before it? How far must a prosecution's evidence extend in order to render potential doubts theoretical or fanciful rather than reasonable? For instance, does the evidence of a store detective as to the operation of a retail point of sale system[23] suffice, or should it require an independent expert report on the system? Or something in between?

51. That assessment may be somewhat instinctive, influenced by informal or unconscious attitudes and assumptions about the reliability of computers generally. If that results in the standard for proof beyond reasonable doubt being set lower than it otherwise might be, the formal evidential presumption may never come into play at all; or at least, the boundary between the two may be difficult to pinpoint.

52. It would therefore, I suggest, be **unrealistic to review the formal evidential presumption in isolation from informal assumptions (conscious or unconscious) about the reliability of computer systems** that may manifest more broadly than the formal presumption, and (perhaps most fundamentally) from consideration of what should constitute proof beyond reasonable doubt in the first place.

Criticisms of the presumption of reliability

53. The basic objection to the rebuttable common law presumption, as applied to computer systems, is simply that it does not reflect reality: programming errors are endemic, and may affect the operation of computer systems in various unpredictable ways. Errors are not limited to software applications and operating systems. They can occur in code embedded in hardware.

54. Moreover (as discussed below) a computer may be operating as designed[24] yet still not produce output that corresponds to the external fact that is sought to be proved.

55. Given the impossibility of proving complete absence of errors, a threshold admissibility requirement to prove that all relevant computer systems are error-free would potentially exclude virtually all computer (and therefore documentary) evidence. A lower threshold

---

[22] However, the prosecution is still likely to have to adduce foundational evidence. See discussion below (para 59 et seq) as to what this may entail.
[23] Cf *R v Shephard* [1993] A.C. 380, a S.69 PACE 1984 case. The finding that the store detective's evidence was sufficient for S.69 purposes was evidently influenced by assumptions about the nature of computer systems: "The computer in this case was of the simplest kind printing limited basic information on each till roll." (Lord Griffiths at 387D). The till was connected to a central computer that fed in date, time, customer number and till number on each till roll.
[24] The question of whether a computer is operating as designed is increasingly difficult to determine with AI systems, where the output is not deterministic. See R. Bickerstaff 'Computer-Generated Evidence – Time for a New Approach' (Bird & Bird Insights 19 Feb 2024 www.twobirds.com/en/insights/2024/uk/computer-generated-evidence-time-for-a-new-approach)

inevitably leads into consideration of whether any errors are such as to cast doubt on the reliability of the information sought to be adduced as evidence.

F. THE EVIDENTIAL PRESUMPTION IN OPERATION

The purpose for which evidence is adduced

56. The **admissibility** of computer evidence (including the question of whether it is or is not hearsay) is **inextricably linked to the purpose for which it is sought to be adduced in evidence**. The same information in the same document may be admissible or inadmissible, depending on what is sought to be proved by it.

57. Careful identification of what is sought to be proved is the necessary precursor to determining whether the evidence is real evidence, direct evidence, or hearsay[25]: and whether any necessary foundational evidence is sufficient to support its admission in evidence.

58. That evaluation is conducted at the time of trial (or in a pre-trial hearing), not when the document is created. At least for general purpose computer systems it is unlikely to be possible to predict in advance whether any given computer-produced document is likely to be adduced in evidence at some point in the future, and in order to prove what (in contrast with the output of dedicated forensic tools deployed at the time of investigation or evidence preparation).

The presumption and foundational evidence

59. Although **real evidence** is admissible, it requires **foundational evidence** to **establish its provenance, chain of custody and authenticity**. That applies to computer evidence as much as to any other variety of real evidence – but does not necessarily touch on reliability. Proof of authenticity might have to address risk of tampering or hacking, but not underlying software errors affecting the accuracy of the information contained in the system: computer evidence can be authentic but wrong.

60. However, foundational evidence is not always that limited. Given the enduring importance in criminal proceedings of the rule against hearsay, **foundational evidence** also has to provide **sufficient information about the computer system to enable the court to determine whether the output to be relied upon is real evidence or hearsay (and if hearsay, whether an exception is applicable)**.

61. The court would, for instance, have to know (or at least be able to infer with confidence) whether relevant data input to the system came from a human being or was automatically recorded with no human involvement. In some cases both might be possible (consider a till system where transactions were mostly the result of barcode scans, but some data might be manually input - for instance if an item could not be scanned.[26]) If there was some human involvement, was it such that the data supplied to the system 'passed through a human mind'? (*R v Spiby* (1990) 91 Cr.App.R. 186 (C.A.); *R v AEB* [2024] EWCA Crim 1320)

---

[25] See generally, *Twist v R* [2001] EWCA Crim 1143.
[26] See also *R v McCarthy et al* [1998] RTR 374, C.A. at p.378.

62. If the foundational evidence does not provide the court with sufficient information to be able to make that determination, the computer output will not be admissible (*R v Cochrane* [1993] Crim LR 48; considered in *DPP v McD* [2016] IESC 71). The question of what kind and degree of human involvement renders the output hearsay may be keenly debated. Thus the Irish Supreme Court judgment in *DPP v McD* included extensive discussion of the kind and degree of human involvement that would transform real evidence emanating from a CCTV system into hearsay[27]

Proof of presence or absence of information?

63. A distinction should be made between **proof of a transaction** and **proof of absence of a transaction**[28]. The former is a question of the accuracy of transactions shown in the output. For the latter, the question of reliability goes further: the output should not only be *accurate* in the data that is present, but constitute a *complete record* of events.[29]

64. There could be many possible technical reasons for dropped transactions. If the evidential presumption were to be deployed to assist in proving absence of a transaction, it would most likely be filling a larger gap than it would for presence of a transaction, consequently doing much more evidential work.

65. Where what is relied upon is presence of transactions, in some circumstances the possibility of material error may appear to the court, in the factual context of what is sought to be proved, to be inherently implausible. Thus in *R v Blackburn, R v Wade*, a case on admissibility of invoices and stock records, Henry J observed:

> "The merit (or lack of it) of this point can be readily appreciated if one attempts to envisage first a computer malfunction which substitutes an entirely different set of serial numbers to those which it is instructed to enter on the invoices, and second, the coincidence that would be required for such spurious serial numbers happening to match the serial numbers of the stolen computers identified by Mr Morrisby. In our judgment there is no chance of a computer malfunction achieving that result."

G. RELIABILITY OF COMPUTER OR RELIABILITY OF OUTPUT?

66. The question of computer reliability is different from, but related to, the question of whether the output can be relied upon. The ability to rely on output may in turn vary, depending on what is sought to be proved.

67. In some cases what is sought to be proved is the mere presence of the data itself (e.g. presence of CSAM, or of infringing software, on a seized device).

---

[27] The question of whether output with an element of human input is or is not hearsay will also depend crucially on what is sought to be proven by the output. It is only hearsay if it is relied upon to prove the truth of a statement contained in the document. Thus, for instance, if all that is sought to be proven is the fact of the statement having been made, not its truth, then it will not be hearsay.

[28] In some cases the facts sought to be proved may rely on a combination of presence and absence on the computer record.

[29] Examples include: *R v Shephard* [1993] A.C. 380; *R v Cahill, R v Pugh* Ruling 14 October 2015 DEESLR, 14 (2017) 67; *R v Minors* [1989] 1 W.L.R. 441 (C.A.)*; R v Shone*; (1982) 76 Cr App R. cf. *Archbold*, paras 9.68 to 9-69.

68. The question of evidential reliability is often more concerned with cases in which it is asserted that the output of the system accurately reflects some external event or state of affairs[30].

69. A computer may be working properly, yet its output may not necessarily reflect the external fact sought to be proved (e.g. if an error has been made in manual data entry, or there was an error in a different computer from which data was received, or the lack of congruence was a design feature rather than a bug[31].

70. Conversely, a computer may contain errors, but those are not such as to affect the accuracy of the specific output sought to be relied upon for proof of the fact in question (*DPP v McKeown* [1997] UKHL 4).

71. The same output may be more evidentially reliable for some facts (e.g. the events shown on a CCTV recording) than for others (e.g. the date/time displayed on the recording, which would depend on the source of that information).

72. Dependency on what is sought to be proved in a particular case means that when crafting an evidence regime care has to be taken with notions of the 'correctness' and 'truth' of the output of the computer. Correctness of output is not necessarily the same thing as the truth of a fact stated in the output.

73. Thus inaccurate data might be relied upon to prove existence of a software bug. In that situation it is the document's falsity, not its truth, that is relied upon[32].

74. Ultimately, information stored on and/or output from a computer is a species of document. The evidential status of a document cannot be determined in isolation from what is sought to be proved by reliance on it[33].

---

[30] Such as the assertion that an apparent shortfall in the Horizon system reflected an actual shortfall (*Hamilton & Ors v Post Office Ltd* [2021] EWCA Crim 577 [20]). Cf. the observations at para [24] of *GIL v Public Prosecutor* [2024] SGHC 287 on the application of the Singapore statutory presumption to data captured by a smart watch: "s 116A(1) of the EA would have led to the court presuming that the report containing the raw Watch data was an accurate reflection of the data actually captured by the Watch at the material time. … What was in dispute was an entirely separate and distinct issue – whether the data actually captured by the Watch was a true and accurate reflection of the appellant's activities between 27 February 2021 and 28 February 2021, ie, whether the appellant was asleep at the material time. The presumption under s 116A(1) did not provide any basis for the court to further presume that the data captured by the Watch, including data pertaining to the appellant's state of sleep at the material time, was accurate in any way."

[31] For instance, the accuracy of the output of a computer system could depend on how it deals with rejected automated data input (e.g. because it fails validation) (cf *R v Cahill*; *R v Pugh* Ruling 14 October 2015 DEESLR, 14 (2017) 67). If the system is designed to require manual correction and re-input of the data, but that does not take place, is the computer 'operating properly' or not (if that be the criterion, as it was under S.69 PACE)? Manual correction of errors was a significant issue in the Horizon litigation, addressed as a question of the 'robustness' of the system (summarised at paras 18 to 20 of the CCRC's 28 January 2021 submission to the Post Office Horizon IT Inquiry). Equally the system may be designed to be good enough for everyday purposes, accepting the possibility of less than perfect accuracy.

[32] Staughton L.J. made this point in relation to defamatory statements in *R v Rock* (1994) WL 1060598 (C.A.).

[33] See also R. Pattenden *Machinespeak: section 129 of the Criminal Justice Act 2003* Crim L.R. 2010, 8, 623-637.

H. REGIMES FOR COMPUTER EVIDENCE

75. As the title of my 1994 article *When is a computer not a computer?* suggests, any regime that sets out to make special rules for computer evidence – especially if, like Section 69 PACE, non-compliance creates an absolute bar to admissibility - has to answer the question: **what constitutes computer evidence?**

76. One aspect of the underlying problem (which is alluded to in some observations contained in the Call for Evidence) was encapsulated by the Court of Appeal in *R v Blackburn, R v Wade* (The Times, 1 December 1992):

> "… while it is not necessary for our decision in this case, we would be extremely reluctant to accept that a document produced on a word processor (rather than on a typewriter or by a quill pen) thereby becomes a document to which section 69 applies, that is to say a document produced by a computer rather than a document produced by the writer. If such documents were covered by section 69 then the welcome reforms found in section 24 of the Criminal Justice act 1988 will be greatly diminished and marginalised. Now, with the almost universal use of word processors, if that were to be the case, almost every business document would then become subject to section 69. We cannot believe that that was Parliament's intention when it passed that statute."

77. If that was a troubling issue in 1994, it is far more so now when hardly any documents (not just business documents) are untouched by the digital hand of a computer. **Any special regime for computer evidence would have to grapple with the question of whether it is to apply to all documents in which computers have played a part in their generation, copying, conversion, storage or transmission; and if not, how should the dividing line be drawn?** A particular concern with special regimes for computer evidence is that they have the potential to generate satellite disputes over definitional issues[34].

78. Steyn J. in *R v Minors, R v Harper* [1989] 2 All ER went as far as to suggest that where a computer is merely used to perform functions of calculation, "It is probably right to say that such calculations do not constitute evidence in any strict sense of the word."

79. In the context of a debate about real evidence versus hearsay, McKechnie J. in the Irish case of *DPP v McD* [2016] 71 said:

---

[34] Thus the Baroness Kidron et al amendment refers to: "produced by or derived from a computer, device or computer system". The Report Stage version provides for consideration of error logs. Are error logs themselves also documents 'produced by or derived from a computer"? The article *Recommendations for the probity of computer evidence* (above) suggests a two stage disclosure approach, which would apply where the reliability of computer data is challenged "on reasonable (as distinct from fanciful) grounds". That threshold condition could raise the question of how the court should go about distinguishing reasonable from fanciful at the first stage, and whether that would in practice involve making similar kinds of judgements about the likelihood of error, with implicit assumptions about reliability, to those that have already proved problematic. The Baroness Kidron et al amendment proposed to delegate that evaluation to Rules of Court.

> "I very much doubt the utility of a court having to decide whether a particular appliance is or is not a computer, an issue I suspect that many authoritative figures could argue about long and hard."

80. A dedicated computer evidence regime would require some way of sifting out **innocuous and everyday documents** (as the Call for Evidence suggests for emails, text messages and the like). Whether categorising simply on the basis of type of document or kind of system is the best approach would need careful consideration. Computer errors are not the province solely of bespoke accounting systems and the like. All kinds of system are susceptible to error, for many kinds of reason; and errors are capable of cropping up in any context.

81. Conversely, context (including what is to be proved) can affect whether error is perceived as likely. In *R v Blackburn, R v Wade* (para 65 above), it was not the innocuous or everyday nature of invoices and stock records that rendered computer error inherently implausible, but the context of what specifically was to be proved by those documents[35][36].

82. If, as suggested in *R v Blackburn, R v Wade*, a word processor should be treated not as a computer-produced document, but as the equivalent of a quill pen, should a spreadsheet be treated as the equivalent of a slide rule? Would that apply both to the spreadsheet program itself and the (often highly complex and error-prone) formulae written and entered by users? Conversely, would a special computer evidence regime apply to all of the spreadsheet, the spreadsheet program, the operating system, the communication system via which it was distributed, and any other systems that touched it? If so, would the same apply to word processed documents?

83. There is a real prospect (as the Call for Evidence acknowledges) that a computer-specific regime could end up throwing too wide a net and, through imposition of unrealistic requirements, exclude evidence that ought to be admitted. The challenge for any computer-specific evidential regime of finding principled and workable dividing lines according to type of output or type of system is a formidable one. Other criteria would most likely also fall to be considered.

---

[35] However, assessments of inherent implausibility require care. It might be argued that because a system is generally reliable, no error is likely to have occurred in the instant case and the output can be relied upon. That, however, is rather like concluding that because the chances of being struck by lightning are minute, the charred body under the tree must be the result of foul play. That confuses the chances of any one individual being struck by lightning with the chances of someone, somewhere being struck by lightning - which is in fact quite common: "30 to 60 people are struck by lightning each year in Britain and, on average, three people die". www.britishrowing.org/wp-content/uploads/2020/08/Safety-Alert-Lightning-August-2020.pdf. (See also the evidence of the defence expert noted at 366g of *R v Abadom* [1983] 1 All ER 364.)

[36] It may also be pertinent to note that requests for communications data under Part 3 of the Investigatory Powers Act are in the region of 300,000 per year, amounting to around 1,100,000 data items (IPCO Annual Report 2022). A small (~0.1%) but nonetheless significant (in terms of the impact of some of the errors, such as search warrants executed against innocent people) proportion of those requests produce erroneous data, for a variety of reasons such as mistyped IP addresses or time zone and daylight saving time errors. The fact that these errors occur rarely (as a proportion of the total number of requests) does not render the possibility of occurrence theoretical or fanciful: almost every year the Investigatory Powers Commissioner reports several such errors that have had serious consequences (see www.cyberleagle.com/2014/07/the-other-side-of-communications-data.html).

THE CALL FOR EVIDENCE PROPOSALS

84. Turning to the **specific items that the Call for Evidence proposes as being in and out of scope of an evidential presumption**:

Out of scope of the presumption[37]	**In scope of the presumption**
Evidence generated by software	***Evidence merely captured or recorded by a device***
Accounting programmes such as the Horizon system used by the Post Office	Digital communications between people such as text messages, messages sent through web-based messaging services, social media posts, e-mails
Automated fraud or plagiarism detection software	Digital photographs and video footage
Automated reporting based on records entered into devices, such as handheld devices for entering patient interactions in a hospital	Breathalyser readouts
	Mobile phone extraction reports

85. On close analysis it is difficult to discern a distinction of principle between the two proposed categories. The professed distinction is between generation and mere capture or recordal. However, if the concern about the evidential presumption of reliability is that all software is inherently prone to errors, it is difficult to understand the rationale for a distinction between generation and recording. Both are highly likely to involve software, and a programming error is capable of affecting output from either kind of process[38].

86. The 'generated v captured/recorded' distinction proposed by the Call for Evidence bears some superficial similarities to the hearsay versus real evidence distinction (albeit that on the particular facts of a case, and depending on what was to be proved, different answers to the question of real evidence or hearsay might be given for the same computer output). However, it is difficult to see how, given the pervasiveness of digital devices for both generation and capture and recording, that distinction necessarily assists in answering the question of whether a given computing device should or should not be assumed to be reliable.

87. In any event, there are difficulties in fitting the given examples into the proposed overarching 'generated v captured/recorded' division:

88. First, what distinction of principle is being drawn between **digital communications** (said to be captured or recorded) and **manual entry of patient interactions into a handheld device at a hospital** (said to be generated)? Both involve a human being entering information into a computer system. Both are dependent on software and hardware, and potentially subject to various kinds of error.

---

[37] The Call for Evidence describes these as being in scope of reform.
[38] Cf the famous example of a well-known brand of photocopier changing numbers. www.independent.co.uk/tech/you-couldn-t-make-it-up-blogger-identifies-numberchanging-glitch-in-xerox-copying-machines-8749076.html

89. If the distinction drawn is between the data entered and reports based on that data, would that mean that an automated report based on data entered into the hospital handheld device would be in scope, but that the underlying entered data would be treated as 'merely captured or recorded' and thus out of scope? The 'mere capture or recordal' of the external data is, of course, itself done by a computer system. The data would then be transmitted to another computer system (or through a series of systems)[39].

90. Second, the proposed categories are silent as to how word processed or copied and scanned (with or without OCR) documents would be treated (and on what principled basis) (see discussion above at paras 76 to 82). The categories are also silent on the infinite variety of other commercially and publicly available software packages that are in use both personally and in business.

91. Third, as regards accounting systems being in scope of reform (and thus out of scope of the presumption), is this meant to refer only to bespoke or heavily customised accounting systems (which would, presumably, include banks[40])? Would it include standard accounting software packages? As mentioned above, how would spreadsheets be treated?

92. Fourth, digital photographs and video footage can come from a variety of different sources: everything from cameras and mobile phones, to dashcams, to CCTV and smart doorbells. As discussed above, the assumptions that it may be reasonable to make about the output will depend, among other things, on what is sought to be proved. There may be a high degree of confidence in the image itself (subject to e.g. a mobile user not having used 'effects' software to alter the image), but the same will not necessarily be true of a date/time stamp displayed on the image, or contained in the metadata. That may require independent verification. (Of course it may not be the output that is erroneous, but an assumption that is made about what it represents.[41])

93. Furthermore, hearsay considerations may come into play: the date/time stamp on a device that takes its time from an NTP (Network Time Protocol) server may be real evidence, whereas a manually entered time may (at least arguably) be hearsay. In the case of e.g. failure to reset manually for summer time, it could be said the computer itself is reliable, even though the output is not an accurate representation of reality.

94. Fifth, breathalysers have, of course, in the past been the subject of many challenges to their readouts and a large quantity of caselaw. The Lion Intoximeter was the subject of *Castle v Cross*, Div Ct [1984]) and the presumption has been routinely applied in breathalyser cases for many years.

---

[39] As was the case in *R v Cahill*; *R v Pugh* Ruling 14 October 2015 DEESLR, 14 (2017) 67.
[40] Cf. P. Marshall 'English law's evidential presumption that computer systems are reliable: time for a rethink?' *Butterworths Journal of International Banking and Financial Law* July/August (2020 Vol 35 – No. 7).
[41] See, for instance, this discussion of the 'created date' in a video clip. https://insights.doughtystreet.co.uk/post/102k7i0/telephone-evidence-in-criminal-proceedings-tactics-strategy.

95. Sixth, it is not obvious what 'mobile phone extraction reports' refers to. Is the computer in question the forensic tool used to extract the data from the phone, or the phone itself, or perhaps both? Should a forensic tool developed specifically for use in investigation and prosecution of offences necessarily be treated in the same way as a general purpose computing device from which the data is extracted? (see discussion at paras 99 to 101 below).

96. On that point, there is an interesting comparison with *R v Wood* [1982] EWCA Crim J0628-2. In that case substantially the same analytical tools were used in the course of a business to measure, calculate and record the composition of samples of manufactured metal, then much later to perform comparative tests on samples suspected to be stolen. Both sets of results were held admissible, but on different bases. Comprehensive evidence was adduced from not only the chemists who performed the analysis, but from the person who programmed the software used to calculate the results[42].

I. DISCUSSION

97. Perhaps, rather than seeking to craft rules predicated on a bright line distinction between whether a document is or is not produced by a computer, consideration should be given to incorporating safeguards, where appropriate, into **a regime generally applicable to documentary evidence**. Even then, as can be seen from the old caselaw on Section 69 PACE noted below, the interaction of any such regime with (in particular) rules on admissibility of hearsay evidence would require careful consideration.

98. Consideration would have to be given to whether the requirements of any special regime for computer evidence were intended to be **a self-standing route to admissibility or additional requirements for evidence that would otherwise be admissible**. That was an issue in relation to Section 69 PACE (see discussion below)[43].

99. There may also be a distinction to be drawn between on the one hand, **forensic tools** used by investigators and prosecutors to acquire, process, analyse and present the contents of computers (e.g. from seized devices), and on the other hand the reliability of the source computer data thus acquired.

100. Most forensic tools will now constitute, or at least contain, computer programs. Often, those tools will have been developed specifically to support the investigation and prosecution of crime. As such, their reliability and proper use in the case at hand ought in principle to be capable of some degree of proof.[44] [45]

---

[42] Professor Peter Sommer's submission to this Call of Evidence includes examples of investigators using both dedicated forensic tools and general purpose capture software.
[43] And see fn 2 above in relation to the Baroness Kidron et al proposed amendment.
[44] How far such proof should go, at least for a new tool, is a topic in its own right: should, for instance, the source code be made available for checking? The 'incremental development' approach described by Lord Widgery CJ in *Campbell v Wallsend* could in principle be applicable to specific forensic capture, extraction, analysis and court presentation tools. However, see the Response of Professor Peter Sommer to this Call for Evidence (especially para 13) for (inter alia) the difficulty in establishing a stable baseline for any presumption of reliability. The use of such tools would invariably be supported by expert evidence, providing the opportunity for cross-examination.
[45] This is not invariably the case. As noted above (para 96) in *R v Wood* the analyses of seized processed metals performed for the purposes of the prosecution utilised substantially the same tools

101. By contrast, the data that has been acquired and processed will typically have come from **general purpose software and devices**, or from other systems that are not designed specifically to support criminal prosecutions[46]. That creates a dilemma: to demand strict proof of the reliability of all such data, in all circumstances, may impose an unfeasible burden on the prosecution and fail to achieve justice in cases where a conviction ought to result; yet not to have any safeguards risks miscarriages of justice through reliance on erroneous information[47].

102. One possible point of distinction might be **whether the information sought to be adduced is central to the prosecution case and/or whether it is corroborated by other evidence**[48]. The potential relevance of centrality to the evidential presumption is discussed above. As to corroboration, it is noteworthy that the key determinant of which Horizon appeals were allowed by the Court of Appeal was whether the Horizon evidence was uncorroborated[49].

103. I am doubtful whether a general distinction between 'simple' and 'complex' devices would be capable of setting a criterion capable of clear application. The evidence required to enable a court to make a determination might itself be extensive.

Concrete hypotheticals

104. Whatever scheme may be proposed for admissibility of, or reliance on, computer evidence, it would be crucial to understand how it would operate in the real world of the criminal courts. That understanding would have to be both concrete "How would it operate in this case?" and principled "Why would applying the scheme have this outcome in this case?".

105. Those questions could only be fully answered by testing any proposed scheme against **concrete factual hypotheticals** - of which caselaw provides a rich collection. A proposed regime could be tested against at least the following (in each case, on the alternative assumptions that the accuracy of the computer output was and was not questioned; and on the assumption that the devices featured in the older cases would now be digital):

- The account print-out in *R v Minors* (as evidence of absence of entries recorded in a building society passbook).

---

as did the analyses carried out during their manufacture. See also Professor Sommer's Response to this Call for Evidence, paras 20 and 23 to 27.

[46] See the Response of Professor Peter Sommer to this Call for Evidence at paras 11 to 15 and 21 to 24 for the range of source computer data that may be available from general purpose systems.

[47] In many cases, of course, a prosecution expert witness will have access to the whole body of data and programs present on a seized device and be able to give an opinion as to authenticity and reliability of the device's systems in the light of all information recoverable from the device.

[48] The Marshall et al recommendation notes as disclosure factors: "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." P. Marshall et al: *Recommendations for the probity of computer evidence* DEESLR, 18 (2021) 18.

[49] *Hamilton & Ors v Post Office Ltd* [2021] EWCA Crim 577. See also Response of Professor Peter Sommer to this Call for Evidence, para 13.

- The printout from a bus company's season ticket records in *R v Harper* (as evidence that a season ticket was stolen).
- The printout of telephone call data from a hotel's automatic recording system in *R v Spiby* (as evidence of e.g. date, time, duration, room from which the call was made, external number called); and similarly the mobile phone provider's records in *R v McDonald* ([2011] EWCA Crim 2933).
- The invoices and stock records in *R v Blackburn*, *R v Wade* (as evidence of serial numbers matching stolen computers).
- The store till rolls in *R v Shephard* (as evidence of absence, i.e. that items were not purchased).
- The defendant's till roll in *PPS v McGowan* (as evidence of an after-hours sale of alcohol).
- The vehicle manufacturer's computer printouts in *R v McCarthy et al* [1998] RTR 374, C.A. (as evidence of serial numbers of parts incorporated in manufactured vehicles).
- The Dutch bank transfer documents in *R v Boulkhrif* [1999] Crim LR 73 (as evidence of transfers made).
- The ATM transaction records in *R v Cochrane* (as evidence of withdrawals made using a chip and PIN card).
- The retailer gift card records in *R v AEB* [2024] EWCA Crim 1320 (as evidence of transactions involving certain gift cards).
- The credit card records obtained from the Landslide child pornography website database in *O'Shea v City of Coventry Magistrates' Court* [2004] EWHC 905 (as evidence of the defendant accessing the website).
- The stock records in *R v Shone* (1982) 76 Cr App R. (as evidence of absence of entries denoting sales).
- The spreadsheets of mobile phone data obtained from overseas via an MLAT request in *Stokes v R* [2025] EWCA Crim 5.
- The smart watch data in *GIL v Public Prosecutor* [2024] SGHC 287 (as evidence of its wearer's activities).

J. THE RISE AND FALL OF S.69 PACE

106. It has not (as far as I am aware) been suggested that mere abolition of the common law presumption would provide a solution to the difficulties faced by criminal defendants in challenging the reliability of evidence obtained from computer systems. Nor has reinstatement of S.69 been proposed[50]. The most developed proposal combines a disclosure scheme with rules about how reliability has to be proved in the light of the disclosure. As such, unlike S.69 it is not on the face of it a test for admissibility (although might that be a consequence of non-compliance?)[51].

---

[50] Other than as a probing amendment by Baroness Kidron et al to the previous government's Data Protection and Digital Information Bill. The difficulties that arose with S.69 are illustrated by the caselaw summarized below.

[51] P. Marshall et al: *Recommendations for the probity of computer evidence* DEESLR, 18 (2021) 18. The Baroness Kidron et al amendments were framed as a multi-factorial evaluation. They did appear to set threshold conditions for either admissibility (the Committee Stage version) or reliance (the Report Stage version).

107. Nevertheless, the history of the introduction and subsequent repeal of S.69 provides some useful parallels with the debate that has re-emerged 40 years later. Notwithstanding the vastly different computer and online landscape that exists today, the issues with which the legislation had to grapple are familiar.

J. The introduction of S.69

108. What evolved into S.69 PACE 1984 was first proposed more than ten years earlier, in the Criminal Law Revision Committee Eleventh Report of June 1972 (*Evidence (General)*). The Committee's proposal (and indeed the preceding s.5 Civil Evidence Act 1968, on which the proposal was based), was intended to overcome perceived obstacles to the admissibility of computer evidence[52], but subject to conditions:

> "Admissibility is subject to strict conditions, necessary in order to ensure that the information is reliable, as to the regular supply of information to the computer and to its proper working. The section in the [1968 Civil Evidence] Act did not derive from a recommendation of the Law Reform Committee, but was asked for by interested business and professional bodies. It seems to us desirable to include a similar provision in the Bill, because the increasing use of computers by the Post Office, local authorities, banks and business firms to store certain kinds of information will make it more difficult to prove certain matters, such as cheque frauds, *unless it is made possible for this to be done from computers*." [para 259] (emphasis added)

109. S.69 was a shorter version of the Revision Committee's proposed clause. Furthermore, it inverted the original proposal: the Law Commission had proposed that (as with S.5 Civil Evidence Act 1968) computer evidence would be admissible if it satisfied the conditions. S.69 was in negative form: it provided that it would not be admissible if it did not satisfy them. This change meant that the S.69 conditions were not an independent route to admissibility, but were additional to any other admissibility requirements[53].

110. The Home Secretary at the time of the introduction of S.69, Leon Brittan, observed during the Bill's Third Reading (16 May 1984):

> "In the evidence provisions of the Bill, parts VII and VIII, we have been concerned not only with important matters of principle but also with complex legal and technical questions. As a result of wide consultation about the impact of high technology on material available to the courts, we have been able to simplify considerably the provisions relating to the admissibility of documentary records and computer evidence, while ensuring that sufficient and stringent conditions are reliably met."

Pre-S.69 cases

---

[52] The perceived obstacles to admissibility were compounded by confusion about the evidential categorisation of computer records, notably a common misapprehension that computer output is necessarily hearsay. That was put to rest in *R v Wood*. A computer record may or may not contain hearsay, depending on how the computer is used, the source of any statement contained in the record and on what is sought to be proved by it.

[53] *R v Minors*, *R v Harper* [1989] 2 All ER 208, at 213.

111. Before the introduction of S.69 criminal caselaw had touched on computer evidence or its precursors. The interactions between real evidence, hearsay and business records were addressed. Some propositions that can be gleaned from those cases are:
- The common law prohibition on admissibility of hearsay evidence in criminal proceedings extended to information transcribed from microfilm copies of index cards by witnesses responsible for keeping the records, but who had not compiled them. (*Myers v DPP*, 1964 (unique number engraved on a car's engine block during manufacture and manually entered on a card index by production staff))[54]
- Where account credits (representing paid-in cheques) were manually entered into a bank's computer system by an operator, printouts of the transactions were hearsay evidence but were rendered admissible under the hearsay exception introduced by the Criminal Evidence Act 1965 (*R v Ewing*, 1983).[55]
- By contrast, information automatically recorded by a mechanical device was real evidence, not hearsay, since it does not record any statement made by a human being. Real evidence is admissible at common law with appropriate foundational testimony. (*Statue of Liberty* ([1968] 1 W.L.R.]).
- Evidence from a computer used to make calculations (as opposed to retrieving stored data) is a species of real evidence (*R v Wood* (1982) (a program written to calculate proportions of metal in ingots based on X-ray spectrometer and neutron transmission readings) [56]. (See also *Castle v Cross* (1984) (Lion Intoximeter).
- Potential for computer error did not render evidence stemming from a computer particularly sensitive, so as to place it into a separate class in relation to admissibility. (*Castle v Cross* (1984) (Lion Intoximeter)).

112. As to the rebuttable presumption *omnia praesumuntur rite esse acta*:

- The presumption is not necessarily to be relied upon as prima facie evidence where the fact to be proved is central to the offence and issue has been taken with it. It is not necessary to provide grounds on which to doubt the fact in question. However, if issue has not been taken that could amount to an admission by the defence. (*Scott v Baker* (1969) (Div Ct) (Secretary of State's approval of Alcotest breathalyser not presumed);
- See also *Dillon v The Queen* (1982) (PC) (Lawfulness of custody not to be presumed in a prosecution for the offence of negligently permitting a prisoner's escape from lawful custody: "It is well established that the courts will not presume the existence of facts that are central to an offence" citing, inter alia, *Scott v Baker*).

However, see the discussion at paras 40 to 44 above as to the application of these cases to the presumption of mechanical reliability.

- The presumption of reliability could be applied to computer evidence, where no challenge to the efficiency of an Intoximeter breathalyser machine at trial was

---

[54] Following *Myers* a statutory exception was introduced for statements in business records, subject to various safeguards. (Criminal Evidence Act 1965, *R v Wood* at p.27)

[55] But depending on the precise purpose for which they were adduced in evidence, the print-outs might be real evidence. See commentary by Steyn J. (as he then was) in *R v Minors, R v Harper* at 212e to h. He recognised that there 'will be much room for serious argument whether a print-out does amount to real evidence…".

[56] But see comments of Steyn J at para 78 above as to whether such calculations are evidence at all.

recorded and the justices made no finding which would permit the inference that the machine was in any way defective or not in proper working order. It was presumed to be in proper working order and that the proper procedure was followed. The Intoximeter was described as a sophisticated machine which depended for part of its operation on computer control. (*Castle v Cross* (1984) (Stephen Brown LJ)

See the discussion at paras 27 to 31 above as to whether this case supports the proposition that the presumption will automatically be applied to all kinds of computer.

The S.69 era

113. A series of cases followed the introduction of S.69. By the time of its repeal 15 years later in 2000, the following had been established:

- The prosecution had to adduce sufficient evidence to enable the court to decide how to categorise the computer evidence (e.g. real evidence or hearsay) for the purpose of any applicable statutory requirements. (*R v Cochrane* [1993] Crim LR 48*;* see also *DPP v McD* [2016] IESC 71 [56])
- The requirements of S.69 were cumulative with other admissibility requirements (such as for hearsay) (*R v Minors, R v Harper* [1989] 1 W.L.R. 441 (C.A.)).
- The requirements of S.69 applied to documents produced by computer, whether the documents constituted real evidence or hearsay. (*R v Shephard* [1993] A.C. 380)
- Oral evidence of the proper working of a computer system under S.69 did not have to be given by a computer expert. Nor did the evidence have to speak to its internal workings. The evidence could be given by a user of the system, such as a store detective in relation to till receipts produced by a point of sale system connected to a central computer[57]. (*R v Shephard* [1993] A.C. 380)

[57] Although the House of Lords held that evidence did not have to be given by an expert, there might still have been a question to be explored of whether it was realistic to confine oral evidence to factual evidence, and if it strayed into expert opinion (for instance during the kind of lengthy cross-examination noted by the Law Commission) how the duties of an expert would be complied with.