ARTICLE :

Establishing innocence when computer data indicates guilt

By Amy Elkington

Introduction

The Post Office scandal has been widely described as the UK's biggest ever miscarriage of justice.[1] During the period between 1999 and 2015 over 900 people were convicted of theft and false accounting offences. These convictions were based on data from the faulty Horizon IT system. Whilst the statutory Post Office inquiry continues to examine the wide-ranging failings that led to these convictions, one area that deserves consideration is how the repeal of section 69 of the Police and Criminal Evidence Act 1984 (Evidence from Computer Records) enabled these convictions to be possible and whether the section should be reinstated. Following recommendations from the Law Commission in 1997, the presumption that computer evidence needed to be proved as reliable before it could be relied on in court was removed by section 60 of the Youth Justice and Criminal Evidence Act 1999. This returned the law to the common law position that presumed the (faulty) Horizon IT data was taken to be accurate unless it could be proved otherwise. This meant that, in effect, the change in the law reversed the burden of proof. The lack of the disclosure,[2] by the Post Office during the prosecution of the ensuing court cases, meant the data's validity was left unchallenged. This proved to be problematic for the defendants, as they had limited access themselves to the data, and thus were unable to establish that it was unreliable. Resultingly, the sub-postmaster defendants were guilty as they could not prove themselves innocent. In a legal system that is increasingly reliant on digital information re-examination of the law, that deems that the 'computer is always right' unless shown otherwise, is imperative to ensure fair and open justice is achieved. As such, the Ministry of Justice has recently held a call for evidence with a view to determining whether the common law presumption should be excluded for certain types of digital evidence.[3]

This paper starts by examining three examples of when digital tools have been used in criminal investigation, to highlight the dangers of reliance on digital information in the criminal justice system. It then considers the impact of the repeal of section 69 of the Police and Criminal Evidence Act 1984 (Evidence from Computer Records) that presumed computer evidence was inadmissible unless shown to be reliable. This paper argues that a reinstatement of the dictum that 'the computer is always wrong,' unless proved otherwise, is not without its problems and will not resolve the issues that have come to the fore following the Post Office cases. It will be argued that if proper disclosure rules were followed in the Post Office cases, miscarriages of justice could have been avoided without a change in the law regarding the presumption of reliability of digital evidence. This is because proper disclosure would have allowed the reliability of data to be interrogated when assessing its admissibility in court, and its probative value could have been assessed at trial where the burden is innocent until proven guilty. Therefore, instead of a change in the presumption of reliability of digital evidence, this paper will propose that criminal sanction should be introduced for failure to disclose evidence that has been collected for the purpose of criminal prosecution.

[1] See, for example, 'Exposing the driving force of the Post Office scandal' (*UK Research and Innovation*, 7 November 2024) < https://www.ukri.org/who-we-are/how-we-are-doing/research-outcomes-and-impact/esrc/exposing-the-driving-force-of-the-post-office-scandal/#:~:text=The%20Post%20Office's%20Horizon%20scandal,pursued%20by%20the%20Post%20Office>; 'Post office/Horizon Scandal' (*Criminal Cases Review Commission*) < https://ccrc.gov.uk/post-office/>; Ministry of Justice, 'Government to quash wrongful Post Office convictions' (*GOV.UK*, 10 January 2024) <https://www.gov.uk/government/news/government-to-quash-wrongful-post-office-convictions> accessed 5 March 2025.

[2] The duty of the prosecutor to disclose is set out in section 3 of the Criminal Procedure and Investigations Act 1996.

[3] Ministry of Justice, 'Use of evidence generated by software in criminal proceedings: Call for Evidence', (*GOV.UK*, 21 January 2025) <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> accessed 5 March 2025.

This will provide a deterrent to those purposely concealing evidence that is not easily accessible, or even its existence known, to the defence.

Moreover, this paper will argue that the Government's examination of excluding certain types of digital evidence from the common law presumption that the 'computer is always right', would be unworkable in practice. Instead, in acknowledgment of the current, and developing, understanding of the potential for unreliability or manipulation of computerised data,[4] this paper proposes that new guidelines need to be introduced for when digital evidence is presented in court. These guidelines should mirror the approach taken in the Turnbull warning[5] for when eyewitness evidence is relied to identify the defendant in a criminal case.

Use of digital evidence in criminal investigation and the 'Minority Report'

23 years ago, Tom Cruise starred in the film the Minority Report. The film is set in 2054 when an elite crime squad can predict and prevent the crime of murder before it occurs. Thus, by imprisoning those who are about to commit murder it reduces the murder rate to zero. As the plot unfolds, it becomes apparent that the crime prevention system is subject to manipulation and thus flawed. It is quickly abandoned, and all criminals imprisoned under it are granted immediate pardons and are released from prison. This fictional storyline, seems scarily close to the truth when the Post office scandal is considered. As we have seen over the past 25 years, however, the sub-postmasters convicted of crime using the faulty Horizon system have faced a much harder battle to clear their names. Whilst the predicative policing in the Minority Report is based on the ability of three gifted humans to see into the future, one has to ask themselves how far this predicative policing fiction is from today's reality. Moreover, whether there is sufficient regulation and accountability when artificial intelligence and computer data is used to convict people of crime.

There is no doubt that the use of computer data and artificial intelligence can make criminal investigation more efficient. This digital evidence can then be used to support a conviction in court. It is not, however, without the risk of overlooking those who potentially should be charged and prosecuted, or (more worryingly) identifying and prosecuting of those who are innocent. Below, three examples of the use of digital evidence in criminal investigation are explored.

The first example of the use of computer data and artificial intelligence within the criminal justice system in the detection and prevention of crime is Kent Police using an Evidence Based Investigative Tool (EBIT) to assess the solvability of crimes. This tool guides the prioritisation of investigation of high-volume crimes to ensure finite resources are suitably deployed. This, however, led to the NewScientist in 2019 to claim that due to the algorithm police investigated roughly half as many reported assaults and public order offences, with the previous 75% investigation rate reduced to 40%.[6] Nonetheless, subsequent research showed that EBIT almost always accurately identified those crimes that were solvable.[7] Thus, demonstrating that whilst significantly fewer crimes were being investigated this resulted in a more efficient use of resources investigations into minor non-domestic assault and public order cases.[8] Whilst efficient use of resources is important, focussed policing can lead to a vicious cycle where certain areas or communities are being over-policed.[9] In the House of Lords Justice and Home Affairs Committee

[4] For further discussion of this in context of the Post Office cases see, Peter Bernard Ladkin, 'Robustness of Software' Digital Evidence and Electronic Signature Law Review, Vol 17 (2020) 15, and James Christie, "The Post Office Horizon IT scandal and the presumption of the dependability of computer evidence" Digital Evidence and Electronic Signature Law Review, Vol 17 (2020) 49.

[5] *R v Turnbull* [1977] QB 224.

[6] Joshua Howgego, 'A UK police force is dropping tricky cases on advice of an algorithm' (*NewScientist*, 8 January 2019), <https://www.newscientist.com/article/2189986-a-uk-police-force-is-dropping-tricky-cases-on-advice-of-an-algorithm/> accessed 5 March 2025.

[7] Kent McFadzien, Alan Pughsley, Andrew M Featherstone, John M Philips, 'The Evidence-Based Investigative Tool (EBIT): a Legitimacy-Conscious Statistical Triage Process for High-Volume Crimes' Vol 4 (2020) Cambridge Journal of Evidence-Based Policing 218.

[8] Kent McFadzien, Alan Pughsley, Andrew M Featherstone, John M Philips, 'The Evidence-Based Investigative Tool (EBIT): a Legitimacy-Conscious Statistical Triage Process for High-Volume Crimes' Vol 4 (2020) Cambridge Journal of Evidence-Based Policing 218, 230.

[9] A term used where the police presence is disproportionate to the amount of reported crime.

first report of the 2021 to 2022 session, 'Technology Rules? The advent of new technologies in the justice system',[10] evidence was provided by Liberty. They argued that the over-policing of one area leads to an increase in the amount of crimes detected. This leads the tool to identify the area as a high crime location, which in turn leads to the recommendation for more predicative policing. Hence, the vicious cycle.[11] As such, this focus on certain geographical areas has the potential to lead to disproportionate and discriminatory policing and prosecution.

The second example of the use of digital technology in policing is the HART (Harm Risk Assessment Tool), used by the police in Durham to assess the risk of arrested persons from committing future offences. The machine-learning algorithm, was used to classify people arrested on suspicion of an offence as high, moderate or low risk of committing a crime in future.[12] Individuals who were assessed as 'moderate' risk were eligible to undertake a rehabilitation programme, and if they successfully completed this, they avoided being charged and prosecuted. Individuals who were assessed as 'high' risk were not eligible to diversion from prosecution. Figures obtained by Fair Trial in 2022 under a freedom of information request showed that 12,200 people were assessed by HART 22,265 times between 2016 and 2021, with 3292 people assessed as high-risk.[13] Evidence showed that the percentage of people being assessed as high-risk by HART was higher than the percentage that would have been classified as such by the police.[14] The problem, was that crude and discriminatory data sets (such as the person's postcode), bought from Experian, were used to come to these conclusions. This continued even though Durham police had been made aware of the potential for bias in 2017.[15] Thus, again demonstrating the dangers of relying on digital evidence in decision making.

The third, and final example, is facial recognition software. This is a digital investigative tool used across all 43 police forces in England and Wales. Retrospective facial recognition has been used for over 100 years. It operates by matching an identified potential offender to images held on a database. The use of current technology means that an offender can be identified in the average time of 5 minutes, which previously had taken up to 10 days when completed manually.[16] More controversially, live facial recognition is used by police to monitor and identify potential criminals, and vulnerable people. It has previously been estimated that the software can scan up to 50 faces per second.[17] The system operates with the real time capture of moving images via CCTV, for example of a location or event. The software that detects individual faces then turns them into numerical values and compares the numerical facial values from the footage to the values om a watchlist.[18] Unlike retrospective facial recognition, this is not targeted. One key concern is that the CCTV images being relied upon can be manipulated by artificial intelligence. For example, algorithmic error correction can be built into CCTV systems, so that missing parts of an

[10] Justice and Home Affairs Committee, *Technology rules? The advent of new technologies in the justice system* (HL 2021-22, 180 - 1).
[11] Justice and Home Affairs Committee, *Technology rules? The advent of new technologies in the justice system* (HL 2021-2022, 180 - 17-18).
[12] Science and Technology Committee, *Algorithms in decision-making inquiry* (HC 2017-19, 351 – 13-14).
[13] 'FOI reveals over 12,000 people profiled by flawed Durham police predictive AI tool' (*Fair Trials*, 15 August 2022) https://www.fairtrials.org/articles/news/foi-reveals-over-12000-people-profiled-by-flawed-durham-police-predictive-ai-tool/ accessed 11 March 2025.
[14] Written evidence from Sheena Urwin to the Parliamentary Committee on evidence on algorithms in decision-making (February 2018) https://committees.parliament.uk/writtenevidence/86851/pdf/#:~:text=The%20purpose%20of%20the%20HART,deferred%20prosecution%20may%20be%20suitable accessed 11 March 2025.
[15] 'FOI reveals over 12,000 people profiled by flawed Durham police predictive AI tool' (*Fair Trials*, 15 August 2022) https://www.fairtrials.org/articles/news/foi-reveals-over-12000-people-profiled-by-flawed-durham-police-predictive-ai-tool/ accessed 11 March 2025.
[16] Chief Inspector Scott Lloyd, 'Key Issues for Policing Supported by AI' (Westminster Legal Policy Forum: Next steps for AI technology in the criminal justice system, online, 18 April 2024).
[17] *Bridges v The Chief Constable of South Wales Police* [2020] 1 WLR 5037, 5045.
[18] Justice and Home Affairs Committee, *Technology rules? The advent of new technologies in the justice system* (HL 2021-22, 180 - 15).

image can be constructed artificially. Such evidence can then be presented in court without any obligation to disclose that the image had been manipulated in this way.[19]

There is currently no bespoke legislation to regulate this use of live facial recognition. Instead, there is a mix of common law, privacy law and codes of practice. The Court of Appeal in *Bridges v The Chief Constable of South Wales Police*,[20] in the first case that questioned the use of live facial recognition, found its use was unlawful. The broad nature of the police's power was an infringement under Article 8(1) of the European Convention of Human Rights. The Court found that police's wide discretion in using live facial recognition was not in accordance with the law under Article 8(2) as there was no clear guidance on where the automated facial recognition could be used, and who could be put on a watchlist that the received images were being cross-referenced to.[21] Furthermore, the Court of Appeal found that the police force had not done all it could to fulfil its public sector duty under the Equality Act 2010, as the police force had never investigated whether automated facial recognition had an unacceptable bias on grounds of race or gender.[22] Big Brother Watch's research and campaign to stop live facial recognition states that live facial recognition is not used anywhere else in Europe. Instead, it is used in "more authoritarian states like China and Russia".[23] In the UK, Parliament has never debated its use and to date not a single law uses the term 'live facial recognition.' Moreover, Big Brother Watch's research showed that almost 90% of the time the live facial recognition software employed by the police gave false positives, meaning that between 2015 and the report being published in 2023 there were 2975 people falsely identified.[24]

Therefore, with this risk of bias and error from digital tools being used to detect crime and identify offenders, it is essential that there are robust safeguards in court to allow people wrongly charged to avoid conviction. There should be two key mechanisms for ensuring this. First, the admissibility or exclusion of evidence, based on its reliability, should be determined before the case comes to court. As is discussed below, this is reliant on the appropriate disclosure of evidence, and raises questions as to who should have the burden of establishing the reliability evidence. Second, any evidence that is deemed admissible should be available to be interrogated in the resulting trial, with the acknowledgement that even though it has been deemed as admissible, this does not mean that it is infallible. The two reforms proposed by this paper ensure both these mechanisms can operate fairly to avoid wrongful conviction of the innocent without the need to change the presumption regarding the reliability of digital evidence.

Admissibility of Digital Evidence: Section 69 of the Police and Criminal Evidence Act 1984 (PACE)

Prior to 1999, section 69 of the Police and Criminal Evidence Act 1984 stated the position in regards to admissibility of evidence from computer records. It stated:

(1) In any proceedings, a statement in a document produced by a computer shall not be admissible as evidence of any fact stated therein unless it is shown—

a) that there are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer;
b) that at all material times the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents…

[19] Justice and Home Affairs Committee, *Technology rules? The advent of new technologies in the justice system* (HL 2021-22, 180 - 16).
[20] [2020] 1 WLR 5037.
[21] [2020] 1 WLR 5037, 5061.
[22] [2020] 1 WLR 5037, 5079.
[23] 'Biometric Britain: The Expansion of Facial Recognition Surveillance' (*Big Brother Watch*, 23 May 2023) < https://bigbrotherwatch.org.uk/wp-content/uploads/2023/05/Biometric-Britain.pdf> 22, accessed 11 March 2025.
[24] 'Biometric Britain: The Expansion of Facial Recognition Surveillance' (*Big Brother Watch*, 23 May 2023) < https://bigbrotherwatch.org.uk/wp-content/uploads/2023/05/Biometric-Britain.pdf> 20, accessed 11 March 2025.

This section was flawed in many ways. For example, a computer can be 'operating properly', meaning that it is not physically broken, but the data provided will only be as reliable as the data set entered. This means the evidence it produced can be widely inaccurate. Moreover, whilst it placed a burden on the person relying on the computer evidence to show that there are no reasonable grounds for believing it was inaccurate, this was arguably an easy burden to discharge. In *R v Shephard*[25] the House of Lords stated that the nature of the evidence required to discharge the burden of showing there had not been improper use of the computer, and that it had been operating properly, would vary in each case. In *Shepherd*, where the computer was a simple one printing out basic information on a till roll, it was deemed that the store detective was fully qualified to give the evidence of its reliability required under s.69(1). There was no need for her to be a computer expert. This lack of requirement to have a person with technical expertise to give expert evidence on complex technology lead Christie to argue that "Lord Griffiths thereby settled the interpretation of section 69, rendering it ineffective as a safeguard".[26] Moreover, computer expert, Turner made the observation that: "This decision has dismantled what had previously been considered to be a well-balanced set of evidential hurdles. Instead, the law will in future follow the dictum 'it's been printed by a computer, so it must be true".[27] Despite these criticisms, the judgment in *Shephard* was followed in *DPP v McKeown*[28] when the House of Lords stated, in the context of an inaccurate clock on an intoximeter, that section 69 was only concerned with the proper operation and function of a computer and not the accuracy of the information supplied to the computer or the truth of the statement it produced.[29] This meant that wide-ranging digital evidence could be admissible at trial, even if it was not necessarily reliable. Thus, as stated by Lord Hoffman in *DPP v McKeown*: "The purpose of section 69, therefore, is a relatively modest one. It does not require the prosecution to show that the statement is likely to be true. Whether it is likely to be true or not is a question of weight for the justices or jury".[30] This meant that issues with the accuracy of data would be left to be challenged during the trial. The relative ease in which the admissibility hurdle could be jumped, meant more importance was placed on being able to effectively interrogate the evidence produced to determine its accuracy. This could mean that a defendant, as in the Post Office cases, would need extensive access to complex information on how the digital evidence was arrived at to be able to challenge the evidence being presented to establish their guilt.

Law Commission's proposals and section 60 of the Youth Justice and Criminal Evidence Act 1999

Against the context of the ineffectual application of section 69 of the Police and Criminal Evidence Act 1984 as a bar to admissibility of unreliable evidence, it is unsurprising that shortly after the judgments of *Shephard* and *McKeown* the Law Commission proposed the repeal of this law. This was achieved through section 60 of the Youth Justice and Criminal Evidence Act 1999. The result was that whatever little protection section 69 of the Police and Criminal Evidence Act 1984 could offer, was now extinguished.

This reform originated from Law Commission's report in 1997 on the use of evidence in criminal proceedings,[31] which was a response to a reference by the Secretary of State for the Home Department in 1994. The reference itself was in answer to the Royal Commission on Criminal Justice.[32] The Law Commission stated that "the use of computer evidence should not be unnecessarily impeded…"[33] and that "section 69 of PACE be repealed without

[25] [1993] AC 380.
[26] James Christie, 'The Law Commission and Section 69 of the Police and Criminal Evidence Act 1984' Digital Evidence and Electronic Signature Law Review, Vol 20 (2023) 62, 71.
[27] Michael Turner, 'Is computer always right?' (*The Lawyer*, January 1993) https://clarotesting.files.wordpress.com/2023/07/michael-turner-letters-to-computer-weekly-the-lawyer-and-computing.-january-1993.pdf> accessed 11 March 2025.
[28] [1997] 1 WLR 295.
[29] [1997] 1 WLR 295, 302.
[30] *DPP v McKeown* [1997] 1 WLR 295, 302.
[31] Law Commission, *Legislating the Criminal Code: Evidence in Criminal Proceedings: Hearsay and Related Topics* (Law Com No 245, 1997).
[32] Home Office, *Report of the Royal Commission on Justice* (Cm. 2263, 1993).
[33] Law Commission, *Legislating the Criminal Code: Evidence in Criminal Proceedings: Hearsay and Related Topics* (Law Com No 245, 1997) para 13.3.

replacement"[34] so that "a common law presumption comes into play: In the absence of evidence to the contrary, the courts will presume that mechanical instruments were in order at the material time".[35] They concluded that:

> We are satisfied that section 69 serves no useful purpose. We are not aware of any difficulties encountered in those jurisdictions that have no equivalent. We are satisfied that the presumption of proper functioning would apply to computers, thus throwing an evidential burden on to the opposing party, but that that burden would be interpreted in such a way as to ensure that the presumption did not result in a conviction merely because the defence had failed to adduce evidence of malfunction which it was in no position to adduce.[36]

Christie provides a critical analysis of the reasoning provided by the Law Commission, and their use of consultation responses, to reach their conclusion. He argues that "the Law Commission did not understand computers or software, and was therefore unable to see the flaws in its thinking."[37] The falsity in the Law Commission's statement, that a conviction would not result merely from the defence's failure to adduce evidence of a malfunction that they were in no position to adduce, is certainly seen when examining the Post Office convictions. One of the key issues was that the defendants did not have access to the evidence from the software manufacturer Fujitsu to adduce that there had been a malfunction.[38] Even if there had been transparency in what data was available, cost and the lack of legal aid would have been a major barrier to the defence relying on it.[39] Moreover, whilst the Post Office cases have been described as one of the most widespread miscarriages of justice it is not a single occurrence, nor one that is unique to private prosecutions. There are many other examples when computer evidence has been wrongly used to convict the innocent.[40]

Despite these potential flaws, the recommendations of the Law Commission were wholeheartedly accepted by Parliament[41] and came into force by means of section 60 of the Youth Justice and Criminal Evidence Act 1999. This states:

> Removal of restriction on use of evidence from computer records.
>
> Section 69 of the Police and Criminal Evidence Act 1984 (evidence from computer records inadmissible unless conditions relating to proper use and operation of computer shown to be satisfied) shall cease to have effect.

This section returned the law to the common law position that computer evidence is admissible unless the defendant can show it is unreliable. A position that Christie vehemently argues is "naïve and unjustifiable" when considering the way modern computer system operate.[42] Nonetheless, in an unfortunate coincidence, in the same year that faulty Horizon software was being implemented in Post Offices across the UK, the removal of the presumption against computer evidence being admissible unless shown to be reliable was enacted by Parliament.

---

[34] Law Commission, *Legislating the Criminal Code: Evidence in Criminal Proceedings: Hearsay and Related Topics* (Law Com No 245, 1997) para 13.13.

[35] Law Commission, *Legislating the Criminal Code: Evidence in Criminal Proceedings: Hearsay and Related Topics* (Law Com No 245, 1997) para 13.13. This common law presumption is set out in *Castle v Cross* [1984] 1 WLR 1372, 1377B, per Stephen Brown LJ.

[36] Law Commission, *Legislating the Criminal Code: Evidence in Criminal Proceedings: Hearsay and Related Topics* (Law Com No 245, 1997) para 13.23.

[37] James Christie, 'The Law Commission and Section 69 of the Police and Criminal Evidence Act 1984' Digital Evidence and Electronic Signature Law Review, Vol 20 (2023) 62, 74.

[38] *R v Hamilton* [2021] EWCA Crim 577 [18].

[39] James Christie, 'The Law Commission and Section 69 of the Police and Criminal Evidence Act 1984' Digital Evidence and Electronic Signature Law Review, Vol 20 (2023) 62, 92-93.

[40] For example, see the discussion of the Princess of Wales Hospital case in Harold Thimbleby, 'Misunderstanding IT: Hospital cybersecurity and IT problems reach the courts' Digital Evidence and Electronic Signature Law Review, Vol 15 (2018) 11.

[41] Standing Committee Deb (E) 29 June 1999 on the new clause two of the Youth Justice and Criminal Evidence Bill [Lords].

[42] James Christie, "The Post Office Horizon IT scandal and the presumption of the dependability of computer evidence" Digital Evidence and Electronic Signature Law Review, Vol 17 (2020) 49.

The Forensic Science Regulator Act 2021 and Forensic Science Regulator's Code of Practice 2023 creates standards of technical evidence for many areas, including digital evidence. Whilst compliance with the Act and Code helps to ensure the reliability of evidence, non-compliance does not mean evidence is automatically inadmissible. Under the common law presumption, a judge can exclude evidence from a trial if the defendant can produce evidence to show why it should be inadmissible.[43] Whilst this appears to provide a safety net to ensure that unreliable evidence that would affect the fairness of the proceedings is not produced at trial, in reality it may be difficult for a defendant to produce the evidence required for a judge to rule that the digital evidence is inadmissible. This is due to the requirement for disclosure requests in a criminal trial not to be "fishing expeditions."[44] In addition, it raises the previously identified issues of knowledge and cost required to adduce such evidence. This is seen in the Post Office case of *R v Hamilton*[45] when the Court of Appeal's decision to quash 39 convictions of theft and false accounting heavily relied on the evidence that had only been disclosed, several years after the criminal trials of the sub-postmasters, in Fulton's judgment in *Bates v Post Office Ltd (No. 6: Horizon Issues).*[46] Even if the holder of the evidential data is not obstructive to disclosure, knowledge and cost will act as a barrier to the defendant being able to meet the evidential burden to have the computer evidence deemed inadmissible due to lack of reliability.[47]

Reform: The Government's Call for Evidence

Following *R v Hamilton* and multiple other sub-postmaster convictions being quashed,[48] James Cartlidge, Parliamentary Under Secretary of State (Ministry of Justice), was asked in the House of Commons whether there were plans to reassess the legal presumption of reliability of computer evidence. He replied: "We have no plans to review the presumption, as it has wide application and is rebuttable if there is evidence to the contrary".[49] This seems to demonstrate lack of appreciation of the problems with providing evidence to rebut the presumption. Following the media attention of the Post Office scandal, it is unsurprising that more recently the Government has undertaken a call for evidence with a view to determining whether the common law presumption should be excluded for certain types of digital evidence.[50] The exclusion of certain types of digital evidence from the common law presumption raises three key issues, which are examined below.

First, it would need to be determined as to what types evidence would be included and what would be excluded. The Ministry of Justice states that:

> We are keen that any changes to the current common law presumption are carefully defined to only include that evidence which is generated by software, including Artificial Intelligence and algorithms. Some (non-exhaustive) examples of that which we envisage being in scope of such reform include:
>
> - accounting programmes such as the Horizon system used by the Post Office
> - automated fraud or plagiarism detection software

[43] Section 78 of the Police and Criminal Evidence Act 1984 provides that a court can refuse to allow evidence when "the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it".
[44] Paul Marshall *et al* 'Recommendations for the probity of computer evidence' Digital Evidence and Electronic Signature Law Review, 18 (2021) 18, 21.
[45] [2021] EWCA Crim 577.
[46] [2019] EWHC 3408.
[47] Paul Marshall *et al* 'Recommendations for the probity of computer evidence' Digital Evidence and Electronic Signature Law Review, 18 (2021) 18, 21.
[48] See for example, *Hawkes v Post Office Ltd* [2022] EWCA Crim 1197; *Ambrose v Post Office Ltd* [2021] EWCA Crim 1443 and; *Allen v Post Office Ltd* [2021] EWCA Crim 1874.
[49] Kevan Jones, 'Admissibility of Evidence: Computers. Question for Ministry of Justice' (*UK Parliament*, 17 May 2022) < https://questions-statements.parliament.uk/written-questions/detail/2022-05-10/79> accessed 11 March 2025.
[50] Ministry of Justice, 'Use of evidence generated by software in criminal proceedings: Call for Evidence', (*GOV.UK*, 21 January 2025) <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> accessed 5 March 2025.

- automated reporting based on records entered into devices, such as handheld devices for entering patient interactions in a hospital

We believe that evidence which is merely captured or recorded by a device should be excluded. For example:

- Digital communications between people such as text messages, messages sent through web- based messaging services, social media posts, emails
- Digital photographs and video footage
- Breathalyser readouts
- Mobile phone extraction reports[51]

This suggests that some types of digital evidence will be more deterministic than others, and so there is less concern if the common law presumption, that these types evidence are reliable, remains. Nonetheless, as simple computer programmes form part of increasingly sophisticated larger computer systems and networks, "the presumption of determinism has weakened".[52] For example, as discussed above, live facial recognition software relies on CCTV images.[53] These could be classified as digital photographs and video footage, and as such would be excluded from the scope of the proposed reform. As already stated,[54] however, these images can be manipulated by artificial intelligence. This possibility was recognised in Judicial Guidance in 2023,[55] as updated in April 2025,[56] which warns that: "AI tools are now being used to produce fake material, including text, images and video".[57] This demonstrates that as technology develops the line between evidence which is merely captured or recorded by a device and evidence that is generated by software, becomes increasingly unclear. Ultimately, this means that even if the list of captured or recorded evidence itemised above was currently presumed to be reliable, and admissible in court unless shown to be unreliable, this would be harder to justify as technology develops. Thus, it becomes difficult to answer one of the questions posed by the Ministry of Justice's call for evidence, which asks whether evidence generated by software should be within the scope of the reform and whether evidence which is merely captured / recorded by a device should be out of scope?[58] This question cannot be answered by classifying the evidence into types, such as automated fraud software or a digital photo, as the Ministry of Justice has done. Instead it would need to be examined how the digital evidence was gathered or generated. Guidelines would need to be created, and continually updated, for what would deem evidence to be digitally captured or recorded, rather than computer generated. If enacted, this would mean that in every trial this information would have to be scrutinised before it could be determined whether the presumption the evidence was reliable applied or not.

Moreover, this distinction seems to be justified on the basis that some evidence can be deemed as reliable by either the type it is or how it is generated. This is a false assumption. As technology becomes increasingly sophisticated, there is the possibility of unpredictability regardless of the type of digital evidence it produces. As Christie states: "Whatever reforms are needed, they must be based on the premise that computer systems are not inherently

[51] Ministry of Justice, 'Use of evidence generated by software in criminal proceedings: Call for Evidence', (*GOV.UK*, 21 January 2025) <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> accessed 5 March 2025.
[52] James Christie, "The Post Office Horizon IT scandal and the presumption of the dependability of computer evidence" Digital Evidence and Electronic Signature Law Review, Vol 17 (2020) 49, 60.
[53] See text to n 18.
[54] See text to n 19.
[55] 'Artificial Intelligence (AI) Guidance for Judicial Holders' (*Courts and Tribunals Judiciary*, 12 December 2023) https://www.judiciary.uk/guidance-and-resources/artificial-intelligence-ai-judicial-guidance/ accessed 23 April 2025.
[56] 'Artificial Intelligence (AI) Guidance for Judicial Holders' (*Courts and Tribunals Judiciary*, 14 April 2025) https://www.judiciary.uk/wp-content/uploads/2025/04/Refreshed-AI-Guidance-published-version.pdf accessed 23 April 2025.
[57] 'Artificial Intelligence (AI) Guidance for Judicial Holders' (*Courts and Tribunals Judiciary*, 14 April 2025), 7 https://www.judiciary.uk/wp-content/uploads/2025/04/Refreshed-AI-Guidance-published-version.pdf accessed 23 April 2025.
[58] Ministry of Justice, 'Use of evidence generated by software in criminal proceedings: Call for Evidence', (*GOV.UK*, 21 January 2025) <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> accessed 5 March 2025.

reliable, indeed that complex software is inherently unreliable and unpredictable".[59] In its call for evidence the Ministry of Justice asks how they might ensure that any proposed solution is, as far as is reasonable possible, future-proofed?[60] It will be interesting to see the published responses to this question. Nonetheless, if even the device and software is working correctly, currently it cannot be assumed absolute confidence that any type of evidence produced by a computer is reliable, and this will only get harder as technology develops.

Second, even if it could be resolved as to what types of evidence the common law presumption should no longer apply to, the reinstatement of section 69 PACE would be ineffective if it was interpreted in the same way as it was historically. This is because even if section 69 had been available to be relied on for example in the Post Office cases, the House of Lords judgments of *Shephard* and *McKeown* would have meant that section 69 would have made no difference in protecting the defendants against wrongful conviction. The assumption would be that because the Horizon consoles were working, the computer-generated evidence produced would be deemed admissible and reliable, with little interrogation. Thus, even if accounting programmes such as the Horizon system used by the Post Office were excluded from the common law presumption as suggested by the Ministry of Justice, this may not prevent future miscarriages of justice.

Third, the Ministry of Justice's suggestion for reinstatement of section 69 PACE would reignite the original concerns that existed. These included the added cost and time to Crown Court trials when section 69 was raised.[61] To address this Marshall *et al* recommend introduction of a two-stage disclosure test for when the reliability of computer evidence is challenged on reasonable grounds.[62] Stage one would require disclosure by an authorised person who is subject to disclosure obligations of information such as known 'bugs', security processes, relevant system audits, and evidence of reliably managed records.[63] This would address issues as were raised in the Post Office cases, such as defendants being told, and believing, that they were the only people experiencing these problems, and remote users being able to access the system through a 'backdoor' and change data covertly.[64] If any issues are revealed by this initial basic disclosure, then stage two would require that the party seeking to rely upon the computer evidence be required to prove that none of the facts or matters identified might affect the reliability of the material sought to be relied upon.[65] Whilst Marshall *et al* concede that this change may not have prevented the Post Office miscarriages of justice, this reversal in establishing the admissibility of evidence, would provide greater safeguard of those charged of crimes based on computer evidence.[66]

Therefore, the Ministry of Justice's proposal to remove the common law presumption that the 'computer is always right' for certain types of digital evidence, would not resolve concerns about the admissibility of digital evidence. It would create further difficulty and complexity in continually determining which types of digital evidence the presumption applied to and which it did not. Moreover, if the historic interpretation of section 69 of the Police and Criminal Evidence Act 1984 was adopted then the reintroduction of certain types of digital evidence being deemed unreliable unless shown otherwise, would have little effect. Additionally, as the Post Office cases demonstrate, the focus of the problem centres around the disclosure of evidence. Its admissibility cannot be challenged unless is existence is known. The result is that a different approach, such as the two-stage model proposed by Marshall,

[59] James Christie, "The Post Office Horizon IT scandal and the presumption of the dependability of computer evidence" Digital Evidence and Electronic Signature Law Review, Vol 17 (2020) 49, 68.
[60] Ministry of Justice, 'Use of evidence generated by software in criminal proceedings: Call for Evidence', (*GOV.UK*, 21 January 2025) <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> accessed 5 March 2025.
[61] See Law Commission, *Legislating the Criminal Code: Evidence in Criminal Proceedings: Hearsay* (Law Com CP No 138, 1995) para 14.16 discussing *R v Cochrane* [1993] Crim LR 48.
[62] Paul Marshall *et al* 'Recommendations for the probity of computer evidence' Digital Evidence and Electronic Signature Law Review, 18 (2021) 18, 23-25.
[63] Paul Marshall *et al* 'Recommendations for the probity of computer evidence' Digital Evidence and Electronic Signature Law Review, 18 (2021) 18, 24-25.
[64] *Bates v Post Office Ltd (No.6: Horizon Issues)* [2019] EWHC 3408 [155].
[65] Paul Marshall *et al* 'Recommendations for the probity of computer evidence' Digital Evidence and Electronic Signature Law Review, 18 (2021) 18, 25.
[66] Paul Marshall *et al* 'Recommendations for the probity of computer evidence' Digital Evidence and Electronic Signature Law Review, 18 (2021) 18, 25.

needs to be adopted to ensure cost effective and time efficient disclosure. This paper, however, argues that the law could go one step further and introduce a criminal offence for intentionally omitting to reasonably disclose evidence collected for the purpose of criminal prosecution. This would provide a deterrent for non-disclosure and a safeguard from future miscarriages of justice.

Reform: A Criminal Offence of Non-Disclosure

One of the key issues in the Post Office cases was the deliberate lack of investigation and non-disclosure of the Horizon's defects.[67] The importance of adequate disclosure was illustrated in Hamilton's case when, despite many sub-postmasters pleading guilty of false accounting to avoid a conviction of theft, the conviction could be quashed on the grounds of abuse of process where their plea was founded upon non-disclosure.[68] Introducing new procedure rules for disclosure, and placing the burden of proof back on the prosecution to determine the reliability of computer evidence relied upon, would not necessarily address the Post office's "institutional obstinacy".[69] Whilst the Post Office Minister, Kevin Hollinrake, has told the BBC that those responsible for the Horizon scandal "should go to jail"[70] currently there has been no criminal convictions for those responsible for the scandal. Whilst non-disclosure could amount to professional misconduct,[71] it is unclear what crime they would be charged with. The common law offence of perverting the course of justice requires that the defendant does "some act" [72] or "series of acts which had a tendency to pervert the course of public justice".[73] This suggests that a positive act is required for the offence, and that an omission would not suffice. Non-disclosure of evidence can lead to the evidence being inadmissible at trial under section 78 of the Police and Criminal Evidence Act 1984, or the case being stayed for abuse of process.[74] Nonetheless, even though these sanctions could have serious repercussions for the prosecution's case, it is not the same as the deterrent impact of a specific criminal sanction.

An alternative could be to introduce a specific criminal offence for those who intentionally fail to reasonably disclose digital evidence, which has been collected for the purpose of criminal prosecution. Such an offence can be seen in the recently enacted Automated Vehicle Act 2024. This introduces a specific criminal offence of not disclosing required safety information, which if disclosed would reveal a heightened risk that a vehicle in which an authorised automation feature is engaged would be involved in a dangerous incident.[75] Introducing a new offence for failure to disclose digital evidence would need to be carefully framed so as not to place an unnecessary disclosure burden on the party relying on the evidence. Moreover, the over disclosure of unnecessary information to the defendant can just be just as problematic. Flooding the defendant with irrelevant complex digital evidence would add disproportionate time and cost to their case, and ultimately hinder their ability to effectively defend themselves. Thus, an introduced offence would take a normative approach of requiring reasonable disclosure of evidence. The introduction of a new offence could provide a deterrent for intentional unreasonable non-disclosure of digital evidence, and prevent a repeat of the miscarriages of justice seen in the Post Office cases.

Reform: Special Warning when Digital Evidence Used at Trial

Once digital evidence has been disclosed and is deemed admissible in court, the adversarial nature of a criminal trial enables the weight of the evidence to be interrogated. The presumption of innocent until proven guilty should provide protection for defendants, as it will be for the prosecution to prove beyond reasonable doubt that the

[67] [2021] EWCA Crim 577 [129].
[68] [2021] EWCA Crim 577 [125].
[69] *Bates v Post Office Ltd (No.6: Horizon Issues)* [2019] EWHC 3408 [928].
[70] 'Jail those responsible for Post Office scandal – minister' (*BBC News*, 8 April 2024) https://www.bbc.co.uk/news/business-68760215#:~:text=More%20than%20700%20people%20were,mini%2Dseries%20earlier%20this%20year accessed 11 March 2025.
[71] The Solicitors Regulatory Authority currently has more than 20 live misconduct investigations into solicitors and law firms who were working on behalf of the Post Office/Royal Mail Group. See, 'Statement: Update on the Solicitors Regulation Authority investigation on the Post Office Horizon IT scandal' (*SRA*, 20 February 2025) https://www.sra.org.uk/sra/news/statement-post-office-feb-2025 access 11 March 2025.
[72] *R v Vreones* [891] 1 QB 360, 369.
[73] *R v Cotter* [2003] QB 951, 956.
[74] Criminal Practice Directions 2015 Division 1, section 3C, as amended October 2020. See also, *R v DS* [2015] EWCA Crim 662 and *R v Hewitt* [2020] EWCA Crim 1247.
[75] Automated Vehicle Act 2024, section 25.

defendant is guilty based on the evidence presented. Ladkin *et al* assert that this presumption of innocence should go one step further by arguing:

> a court should start with the presumption that any software system contains or is influenced by errors that make it fallible. It will therefore fail from time to time when a combination of circumstances lead to an erroneous path of execution through the software – and such failures may not be obvious, and may even be perverse.[76]

It is unclear whether Ladkin *et al* are arguing that this presumption should be adopted at the disclosure hearing or the trial stage of the case. Nonetheless, if such an approach were adopted at the trial stage, it would mean that not only was the defendant innocent until proven guilty, but also it would be presumed that the evidence being relied on to ensure a conviction is fallible by nature. This may create an insurmountable hurdle to be overcome in prosecuting defendants, unless additional non-digital evidence is available.

Alternatively, this paper suggests that the approach that is used for eye witness testimony should be adopted for digital evidence. In cases where eye witness testimony is relied upon to identify the defendant, jurors are given additional guidance before reaching their decision, because of the acknowledged unreliable nature of such evidence. This is known as the Turnbull warning.[77] A similar approach should be adopted for digital evidence of providing a warning to jurors when weighing up digital evidence presented at trial.

In cases that really wholly or substantially on eyewitness testimony to identify the defendant, the Turnbull warning requires that:

> the judge should warn the jury of the special need for caution before convicting the accused in reliance on the correctness of the identification or identifications. In addition he should instruct them as to the reason for the need for such a warning and should make some reference to the possibility that a mistaken witness can be a convincing one and that a number of such witnesses can all be mistaken.[78]

Adopting a similar warning for any type of digital evidence would mean that juries would be directed about the unreliable nature of digital evidence, even if the computer is working properly and has no previously reported faults. It would also highlight that digital evidence can be convincing even if it is incorrect and that multiple evidential outputs can all be incorrect even if they agree with each other.

Thus, when digital evidence has been admitted at trial a Turnbull type warning would provide an extra safeguard to the defendant, especially when this is the main evidence being relied on. In effect, it would introduce a requirement that alternative evidence is presented to corroborate the digital evidence, otherwise the prosecution run the risk that solitary digital evidence could be disregarded by the jury. It would acknowledge the fallibility of digital evidence, even when the computer is operating correctly, and provide caution when considering a criminal conviction based on this evidence.

Conclusion

Use of digital tools and artificial intelligence make crime detection and investigation more effective. Algorithms can predict when and where crimes may occur and police forces resources can be deployed more efficiently. Computers, however, are not infallible. Conclusions reached are only as reliable as the data entered. The majority of computers programmes are no longer deterministic and the sophistication of computer systems means that humans cannot reliably predict outcomes.

The Ministry of Justice has called for evidence on a possible reform to address this problem, which would exclude certain types of digital evidence from the common law admissibility presumption that the 'computer is always right'. This reform raises issues of what type of evidence should be excluded and what the requirements would be required for showing that these types of evidence are reliable and thus admissible. Moreover, the Ministry of Justice's

[76] Peter Bernard Ladkin, Bev Littlewood, Harold Thimbleby and Martyn Thomas CBE, 'The Law Commission presumption concerning the dependability of computer evidence', Digital Evidence and Electronic Signature Law Review, Vol 17 (2020) 7.
[77] *R v Turnbull* [1977] QB 224.
[78] *R v Turnbull* [1977] QB 224, 228.

suggestion fails to consider that the presumption of reliability, and who has the burden of proving or disproving it, is not the fundamental issue. Before the reliability of evidence can even be considered, it first requires that this evidence in disclosed. In a world of complex and evolving technology, it may not even be apparent what, if any, evidence exists. Whilst section 3 of the Criminal Procedure and Investigations Act 1996 places a duty on prosecutors to disclose, the large- scale miscarriage of justice that can result when this duty is not followed in evident from the Post Office cases. The introduction of a specific criminal sanction for such failure to disclose could provide one method of deterring unreasonable non-disclosure of evidence.

When digital evidence is deemed admissible in court, the prosecution has the burden of proof in any resulting trial. In all criminal cases the defendant is innocent until proven guilty beyond reasonable doubt. Despite this high threshold for establishing criminal liability, in cases that rely heavily on eye witness testimony to identify the defendant, jurors are warned of the special need for caution. A similar approach should be adopted in cases relying solely or substantially on digital evidence. The jury should be warned of the unreliable nature of digital evidence. Thus, providing further protection for defendants and the avoidance of miscarriages of justice as seen in the Post Office cases.

Dr Amy Elkington, is a Senior Lecturer in Law at the University Chichester, who manages the undergraduate and postgraduate Law programmes. Her specialism is Criminal Law, and she has published a book and several articles in this field.