Use of evidence generated by software in criminal proceedings

Response to consultation, 14 April 2025

Professor Steven Murdoch, University College London

Thank you for the opportunity to contribute to this consultation. My response is not confidential, nor anonymous, and may be published in full or part as the Ministry considers appropriate.

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

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

No

(i) Please specify why you gave this answer

All non-trivial computer systems have bugs, including those known to the developer and those unidentified. It is likely that some of these bugs could cause evidence produced by the system to be unreliable and lead courts to reach incorrect conclusions. In addition, the presumption reduces the incentive for system developers to make use of techniques that will increase the reliability of evidence their systems produce and ease the process of convincing a third party of the reliability of this evidence.

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

In practice, difficult and often impossible.

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

Lack of adequate disclosure

The presumption allows operators of systems to refuse to provide sufficient disclosure to allow parties to adequately challenge the reliability of computer evidence. Even when procedural rules seem to require disclosure, there is sufficient ambiguity in these rules and insufficient penalties for failures of disclosure so operators can ignore these rules in practice, while incurring little risk.

Furthermore, operators of systems may claim that disclosure would be costly or harmful to their interests. If this is the case, it is only the result of the system having been inadequately specified or implemented, because any system that is properly designed to produce evidence can and should allow this to be done cost-effectively and without compromising the integrity of the system.

Difficulties in statistical reasoning

Arguments on the reliability of computer evidence often involve statistical arguments. These may include a numerical basis or could be more qualitative, but in either case, are only valid if carefully reasoned. Computer evidence is particularly at risk of erroneous reasoning since it

involves low probability events, complex dependency relationships and non-normality – all of which require special treatment because intuitive reasoning is liable to result in incorrect conclusions.

Access to expert witnesses

Reasoning about computer evidence will often require expert evidence, and there is a well-known problem in the justice system relating to access to expert evidence, with reasons including lack of access to legal aid and low rates of pay for computer experts.

(i) Please give examples where possible.

The prosecution of Seema Misra is an important example, but the subject of other submissions to this consultation, so I will not go into further detail here. Another case of relevance is Job v Halifax[1], for which I served as an expert witness. The involvement of an expert was only possible because I was acting pro bono, as was Mr Job's barrister, Stephen Mason.

Halifax did not disclose any evidence supporting the reliability of the computer system that produced evidence that was central to their argument that Mr Job was liable for the disputed payment transactions. In fact, Halifax has deleted the detailed logs that would have been of assistance in establishing what had occurred. Halifax furthermore argued that if they disclosed how the system had operated, it could compromise the security of the system.

Instead, Halifax relied on the circular argument that the system is reliable because they assume the large number of disputed transactions reported to them are all customer error rather than system fault, and they can do so because the system is assumed to be reliable. In the absence of convincing technical evidence, the judgment therefore had to rely on the surrounding evidence, such as where the disputed transactions occurred.

2) Are you able to provide examples from other jurisdictions or situations where the reliability of software must be certified?:
a) As examples of good practice?
b) As examples of things to be aware of?

No

3) If the position were to be amended, what in your opinion would be the most appropriate and practicable solution given our aims and objectives set out above? It would be helpful if your answer could address as many of the below as possible:

I support the proposal for handling computer evidence developed by Marhsall et al.[2] and summarised by Bohm et al.[3]

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

I think the proposal, as described, will be effective.

---

[1] Job v Halifax PLC (not reported) Case number 7BQ00307; available in Digital Evidence and Electronic Signature Law Review, Vol 6.
[2] Marshall et al. Recommendations for the probity of computer evidence (2021) https://journals.sas.ac.uk/deeslr/article/view/5240
[3] Bohm et al. Briefing Note: The legal rule that computers are presumed to be operating correctly – unforeseen and unjust consequences (2022). https://journals.sas.ac.uk/deeslr/article/view/5476

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

The proposal is written in terms that are already reasonably future-proofed. It may be accompanied by more detailed guidance that will need to be updated as technology and our understanding of technology advances.

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

The proposal is practical, and based on experience of its use there may be ways to optimise its application through specific guidance developed by experts to apply in commonly occurring situations. This guidance and its application should be regularly reviewed to ensure it is updated, and has not inadvertently led to problems being unidentified.

I would also emphasise that the proposal allows for computer evidence to be shown to be accurate through means that does not require relying on a computer. This technique, known as "Software Independence", may be applicable in some situations and so avoid the need to follow the procedure outlined.

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

In situations where there may be novel issues then PhD-level expertise will be needed. For scenarios that have comprehensive agreed guidance available, and could be considered more routine then ordinary computer expertise may be adequate. In both cases there are sufficient experts available.

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

I would consider evidence in scope if a computer error[4] could plausibly result in the evidence being substantially incorrect or misinterpreted when used in legal proceedings or steps leading up to the proceedings.

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

The reliability of evidence processed by a computer system depends on the reliability of the computer system, regardless of whether the processing is to generate, store or retrieve the evidence. There is no rigorous definition of processing that would allow "generated" evidence to be distinguished from "captured/recorded". In fact, some methods used to store and retrieve evidence are more complex and thus more prone to error compared to some methods used to generate evidence.

In particular, data search/retrieval, and data compression, as used for evidence storage, are some of the most complex algorithms used on computer systems today. For example, a Xerox

[4] Academic literature in software reliability makes a distinction between terms such as bug, fault, error, etc. but I use the term "error" in the widest possible sense to include failures of hardware and software, incorrect specification, and usability failures.

product for storing image files as PDF used a data compression technique which was discovered to change digits of numbers it stores, much to the surprise of its users[5].

As another example, a forensics product specifically designed to retrieve data from smartphones was found to fabricate incorrect timestamp data when the software is unable to find the correct value[6].

Data search software can be designed to prioritise speed over correctness, and so the result of queries may be incorrect in some circumstances. One such example is Elasticsearch, which is explicitly stated to not be reliable in all situations, but still is used for processing computer evidence.

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

Any evidence which has been processed by computer may be in scope, unless it can be shown that there is no reasonable way that computer error could cause the evidence to be incorrect in a material way.

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

Guidance could be developed by experts to handle common scenarios where computer evidence is used in such a way that the risk of material computer error can be safely excluded. Unless such an agreed exception is applicable, then the evidence should be considered in scope.

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

The presumption has allowed some badly managed organisations to create and operate systems that either produce unreliable evidence or produce evidence about which it is not feasible to assess its reliability. If the presumption is removed, it is likely that these organisations will have to modify their systems and procedures relating to computer evidence or find alternative methods to support their arguments in legal disputes. It is entirely possible for organisations to make these changes, and well-managed organisations already do so.

I would encourage the Ministry to resist objections to changes in the presumption from organisations claiming that it is infeasible for them to improve their computer systems or practices. It is in the interest of justice for computer evidence relied upon in court to be accompanied by evidence that this reliance is justified. Any temporary difficulties faced by organisations are a justifiable cost of improving the reliability of computer systems, and so of benefit both to the justice system and society as a whole.

---

[5] David Kriesel, Xerox scanners/photocopiers randomly alter numbers in scanned documents (2013). https://www.dkriesel.com/en/blog/2013/0802_xerox-workcentres_are_switching_written_numbers_when_scanning

[6] Jonathan Zdziarski, An Example of Forensic Science at its Worst: US v. Brig. Gen. Jeffrey Sinclair (2014). https://www.zdziarski.com/blog/?p=3717

About you

Full name:
Professor Steven Murdoch

Job title or capacity in which you are responding to this consultation exercise:
Professor of Security Engineering

Date:
14 April 2025

Company name/organisation (if applicable):
University College London

Address:
Gower Street, London

Postcode:
WC1E 6BT

Email address:
s.murdoch@ucl.ac.uk

What relevant experience / expertise do you have?
Academic; Software Professional; Personal experience of the criminal justice system (Expert Witness)

Biography:
Steven J. Murdoch is Professor of Security Engineering and head of the Information Security Research Group of University College London, working on payment system security, privacy-enhancing technologies, online safety, and the interaction between computer science and the law. He teaches on the UCL MSc in Information Security. His research interests include authentication/passwords, banking security, anonymous communications, censorship resistance and covert channels. He has worked with the OpenNet Initiative, investigating Internet censorship, and for the Tor Project, on improving the security and usability of the Tor anonymity system. His current research is on how computer systems can produce evidence to allow fair and efficient dispute resolution. Professor Murdoch was Chief Security Architect at Cronto, and following their acquisition of the technology he developed, he took on the role of Distinguished Scientist for OneSpan. He is a member of REPHRAIN, the National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online. He is a director of the Open Rights Group, a UK-based digital campaigning organisation working to protect rights to privacy and free speech online and is a Fellow of the IET and BCS.