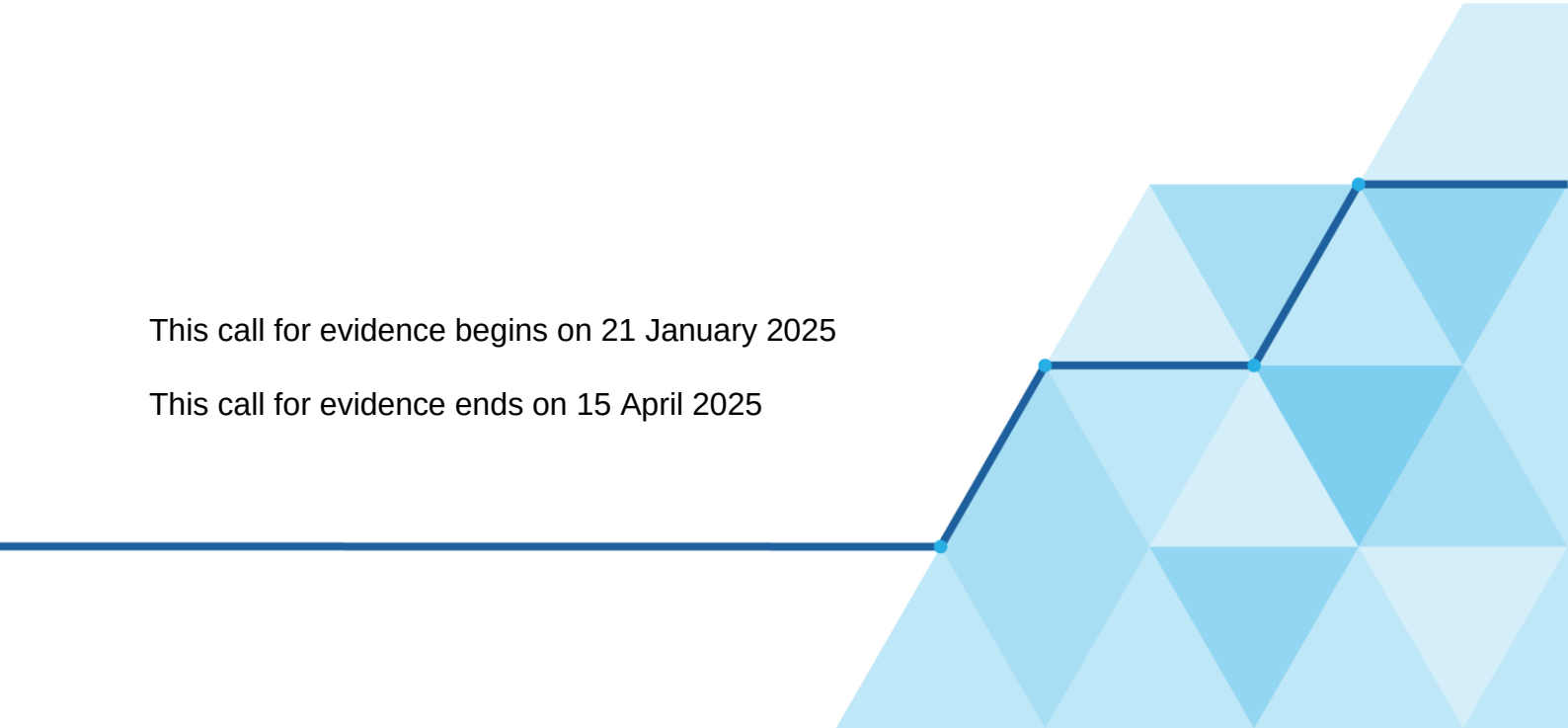
Ministry of Justice

The use of evidence generated by software in criminal proceedings

This call for evidence begins on 21 January 2025

This call for evidence ends on 15 April 2025



The use of evidence generated by software in criminal proceedings

About this call for evidence

To:	All interested parties.
Duration:	From 21/01/25 to 15/04/25
Enquiries (including requests for the paper in an alternative format) to:	Email: computer.evidence@justice.gov.uk
How to respond:	Please send your response by 15/04/25 to: Email: computer.evidence@justice.gov.uk

Contents

Foreword

This Government is committed to a justice system that works for everyone who relies on it, delivering just outcomes in a timely and fair manner.

For that to remain the case, the law and criminal procedure must evolve to reflect the world we live in today.

Current principles around the use of evidence generated by computer software in criminal proceedings were established over two decades ago, with the common law presumption that a computer was operating correctly unless there is evidence to the contrary. In simple terms, ‘the computer is always right’, unless someone can show it is not.

The limitations of this presumption have been highlighted starkly by the Post Office Horizon scandal, which saw hundreds of sub-postmasters wrongly convicted. These convictions were based on evidence which we now know to have been false, due to faults in the Horizon accounting software system, clearly demonstrating the fallibility of evidence produced by software.

Over the twenty-five years since the presumption was last looked at the use of computers and software has evolved beyond all recognition. We live in an increasingly digital and networked world, where software has become highly specialised and complex. The Government believes the time is right to re-examine this important area, to ensure it is fit for purpose.

I welcome the views of all those with an interest in this area of criminal procedure, and hope that your insights will help us to ensure the criminal justice system is fair and effective, both now, and for years to come.

Sarah Sackman KC MP

Minister for Courts and Legal Services

Introduction

This call for evidence is to help us better understand how the current presumption concerning the admissibility of computer evidence is working in practice, and whether it is fit for purpose in the modern world.

The current presumption was introduced in 2000 following a recommendation of the Law Commission following a consultation. Given the use of software and computing systems has increased exponentially in the last 25 years since the Law Commission recommendation, along with changes in the way we use these software systems, we invite views as to whether the time is now right to re-look at this presumption.

Whilst considering this, it is important to note ‘computer evidence’ now proliferates in many prosecutions, particularly in crimes such as fraud, rape and serious sexual offence cases. Computer evidence is also widely used in cases which see high volumes of prosecutions such as driving offences. Therefore it is important when examining this area we consider any ramifications for the effective functioning of the criminal justice system.

It is also vital that, in making any changes to the law in this area, we are clear on how we are defining such evidence, to avoid unintentionally bringing into scope anything which should not be included, or indeed excluding anything which we do consider should be in scope. What constitutes digital evidence could be wide enough to include text messages, social media posts, digitally captured photographs etc. In considering changes to the law relating to the presumption of reliability of such evidence, we consider it important to draw a distinction between this wider digital evidence and evidence which has been specifically generated by a computer system or software.

We welcome views from organisations and individuals with experience of the criminal justice system, along with those with expertise in computers/software and the usage of the evidence generated from them.

Aims and Objectives of the Call for Evidence

Our aim in publishing this Call for Evidence is to increase our evidence base and understanding of the ways in which evidence produced by software is handled in criminal proceedings. This includes how this evidence is treated in other jurisdictions, and any challenges or issues with the current position in this country.

Our overarching objective is to ensure fairness and justice for all those involved in prosecutions.

Our intention is that any proposed reforms will be informed by all available evidence, practicable in the Criminal Justice System as it currently operates, and carefully defined to

give clarity on what is in scope of such reform, and futureproof given the swiftly evolving landscape of technology including the increasing use of artificial intelligence.

Current Common Law Presumption

Prior to 2000 the admissibility of 'computer evidence' was subject to s.69 of the Police and Criminal Evidence Act (1984). This was repealed by s.60 of the Youth Justice and Criminal Evidence Act 1999.

The relevant part of s.69 stated:

> *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 –*
> - *that there are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer;*
> - *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…*

In 1997, following a consultation, the Law Commission published a report recommending s.69 be repealed without replacement. In 2000 it was replaced with a common law (rebuttable) presumption that the computer was operating correctly at the material time. The presumption is a rebuttable one, meaning that if it can be shown that the software may not have been functioning correctly, the burden shifts to whoever is seeking to rely on the evidence to prove that it was.

Proposed scope of any reform to the law

Digital material now proliferates in criminal cases particularly in cases concerning fraud, rape and serious sexual offences. What constitutes digital material has evolved significantly since s.69 was introduced in 1984. If reinstated today, it could now be construed to include everything from the complex accounting software used by commercial banks to text messages, email chains and social media posts.

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,

- 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.

We welcome views on if these are the right boundaries, how these definitions should be drawn, and other examples of specific evidence types which should be in or out of scope.

Questions

We would welcome responses to the following questions set out in this call for evidence.

Questions:

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?
      (i) Please specify why you gave this answer
   (b) How easy or difficult do you believe it is at present for this presumption to be effectively rebutted?
   (c) What barriers do you see in effectively rebutting this presumption?
      (i) Please give examples where possible.

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?

3) **If the position were to be amended, what in your opinion would be the most appropriate and practicable solution given our aims and objectives set out above?** It would be helpful if your answer could address as many of the below as possible:
   a) What procedural safeguards need to be in place to ensure your proposed solution is effective?
   b) How might we ensure that any proposed solution is, as far as is reasonable possible, future-proofed?
   c) How might we ensure that any proposed solution is operationally practical?
   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?

4) **In your opinion, how should 'computer evidence' for these purposes be best defined?**
   a) Do you agree that evidence generated by software, as set out above, should be in scope, and that evidence which is merely captured / recorded by a device should be out of scope? Please provide a rationale for your answer.
      i) Can you provide specific examples of the type of evidence you believe should be in scope?
      ii) Can you provide specific examples of the type of evidence you believe should be out of scope?

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

Thank you for participating in this call for evidence.

About you

Please use this section to tell us about yourself. Please include your answers in your covering email.

Full name
Job title or capacity in which you are responding to this consultation exercise (e.g. member of the public etc.)
Date
Company name/organisation (if applicable):
Address
Postcode
Email address
What relevant experience / expertise do you have? a) Academic b) Practicing legal professional c) Judge d) Software professional e) Forensics expert f) Other relevant professional expertise g) Personal experience of the criminal justice system h) Other
Let us know if you would like us to acknowledge receipt of your response.,
Address to which the acknowledgement should be sent, if different from above.

If you are a representative of a group, please tell us the name of the group and give a summary of the people or organisations that you represent.

Contact details/How to respond

Email: computer.evidence@justice.gov.uk

Complaints or comments

If you have any complaints or comments about the call for evidence process you should contact the Ministry of Justice at the email address below.

computer.evidence@justice.gov.uk

Extra copies

Alternative format versions of this publication can be requested from computer.evidence@justice.gov.uk

Publication of response

A paper summarising the responses to this call for evidence will be published in due course. .

Representative groups

Representative groups are asked to give a summary of the people and organisations they represent when they respond.

Confidentiality

Information provided in response to this call for evidence, including personal information, may be published or disclosed in accordance with the access to information regimes (these are primarily the Freedom of Information Act 2000 (FOIA), the Data Protection Act 2018 (DPA), the General Data Protection Regulation (UK GDPR) and the Environmental Information Regulations 2004).

If you want the information that you provide to be treated as confidential, please be aware that, under the FOIA, there is a statutory Code of Practice with which public authorities

must comply and which deals, amongst other things, with obligations of confidence. In view of this it would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on the Ministry.

The Ministry will process your personal data in accordance with the DPA and in the majority of circumstances, this will mean that your personal data will not be disclosed to third parties.