CPPP/S6/25/18/19

Citizen Participation and Public Petitions Committee
Wednesday 26 November 2025
18th Meeting, 2025 (Session 6)

PE2185: Introduce stronger safeguards around the use of digital material in court proceedings

Introduction

Petitioner	Christopher Simpson
Petition summary	Calling on the Scottish Parliament to urge the Scottish Government to amend the Criminal Procedure (Scotland) Act 1995 to ensure that any digital material presented in court, such as photos or screenshots, is verifiably sourced, time-stamped, and able to be independently authenticated before being considered admissible, unless both parties agree otherwise.
Webpage	https://petitions.parliament.scot/petitions/PE2185

1. This is a new petition that was lodged on 22 September 2025.

2. A full summary of this petition and its aims can be found at **Annexe A**.

3. A SPICe briefing has been prepared to inform the Committee's consideration of the petition and can be found at **Annexe B**.

4. Every petition collects signatures while it remains under consideration. At the time of writing, 149 signatures have been received on this petition.

5. The Committee seeks views from the Scottish Government on all new petitions before they are formally considered.

6. The Committee has received submissions from the Scottish Government and the petitioner, which are set out in **Annexe C** of this paper.

Action

7. The Committee is invited to consider what action it wishes to take.

Clerks to the Committee
November 2025

Annexe A: Summary of petition

PE2185: Introduce stronger safeguards around the use of digital material in court proceedings

Petitioner

Christopher Simpson

Date Lodged

22 September 2025

Petition summary

Calling on the Scottish Parliament to urge the Scottish Government to amend the Criminal Procedure (Scotland) Act 1995 to ensure that any digital material presented in court, such as photos or screenshots, is verifiably sourced, time-stamped, and able to be independently authenticated before being considered admissible, unless both parties agree otherwise.

Background information

I was accused based on screenshots that were never checked for metadata or linked to my device, despite police having my phone and PIN. It was never confirmed who sent them or when they were created. These images could easily have been faked. The impact on my life was severe – I became suicidal and appeared in a documentary on male mental health in Scotland. In today's digital world, anyone can create fake messages. This is not just about my case — it's about fixing a loophole that can hurt anyone. We need proper rules on digital evidence, so courts aren't misled and innocent people are protected.

The action asked for by my petition would not interfere with judicial discretion, but rather provide clearer legislative guidance to protect against the misuse of fabricated or contextless digital submissions, particularly in summary cases.

The motivation behind this proposal is not only my own experience, but related to wider concerns about how easily digital material can be manipulated and misused in the justice system, especially as such material becomes increasingly common in both prosecution and defence submissions.

Annexe B: SPICe briefing on PE2185

Briefing for the Citizen Participation and Public Petitions Committee on petition PE2185: Introduce stronger safeguards around the use of digital material in court proceedings, lodged by Christopher Simpson

Introduction

The petition calls on the Scottish Parliament to urge the Scottish Government to amend the Criminal Procedure (Scotland) Act 1995 to:

"ensure that any digital material presented in court, such as photos or screenshots, is verifiably sourced, time-stamped, and able to be independently authenticated before being considered admissible, unless both parties agree otherwise".

The background information in the petition states that:

"The motivation behind this proposal is not only my own experience, but related to wider concerns about how easily digital material can be manipulated and misused in the justice system, especially as such material becomes increasingly common in both prosecution and defence submissions."

Digital evidence covers any digitally stored or transmitted information (e.g. video footage, photographs, texts, emails, social media posts, computer browser history and GPS date).

Digital evidence may be used in both civil and criminal proceedings. However, given the terms of the petition, this briefing focuses on criminal cases.

Safeguards in relation to evidence

The Crown Office & Procurator Fiscal Service (COPFS) have, in correspondence with SPICe, sought to explain how court procedures currently deal with the authenticity and accuracy of evidence (including but not just digital evidence). They noted that:

"before any item attains evidential status its provenance must be established; an item is meaningless unless its source is in some way proved".

COPFS explained that this can be done through agreement between the prosecution and defence. But where it is not agreed, the side presenting something as evidence must provide a witness to speak to the item. In such situations the other side in the case can challenge the witness and may have their own witness to help rebut what is said.

In the context of digital evidence, the COPFS provided the following illustrative example in relation to a screenshot of text messages:

"Evidence will have to be led, or the provenance agreed, that this is an image of a text conversation between A and B occurring on X date. If it is agreed, then it will go into a joint minute of agreement and read to the jury / handed up to the sheriff. If it is in dispute, then a witness who can speak to its source, usually one of the parties to the conversation, or the police officer who recovered the messages from a phone handset during forensic interrogation of the device, will be required to give evidence."

"The defence will be entitled to challenge the evidence and lead their own rebuttal evidence. Perhaps, in the context of screenprints of a text conversation, if the defence position is that these have been altered, or taken out of context, the defence can produce their side of the conversation showing the complete conversation."

Criminal justice modernisation

The Scottish Government is supporting the development and roll-out of a system for sharing digital evidence in criminal cases. A news release in August 2024 (National roll-out of digital evidence sharing technology) stated that:

"A world-leading £33 million Scottish Government initiative for sharing digital evidence from crime scene to court room is being rolled out across Scotland.

Digital Evidence Sharing Capability (DESC) allows police officers, prosecutors, defence lawyers, court staff and judges to access a secure, unified system to collect, store, process and manage evidence digitally."

The DESC was highlighted in the Policy Memorandum published along with the Criminal Justice Modernisation and Abusive Domestic Behaviour Reviews (Scotland) Bill (passed on 7 October 2025). It noted that:

"Through DESC, digital evidence, such as photographs or video footage, can be shared by members of the public at the point of reporting a crime to the police. This evidence is then shared with the prosecution and the defence agent for the accused in order to allow early consideration and possible resolution of cases. The use of digital evidence through DESC has the potential to improve the experience of victims, witnesses, and the accused in terms of providing swifter justice." (para 64)

The DESC is designed with features intended to preserve the integrity of evidence once it is entered into the system. The above Policy Memorandum stated that:

"assurance can be provided through its automatic audit function which shows every activity on the uploaded file from its receipt to the conclusion of the case". (para 72)

However, these features are not aimed at checking the reliability of digital evidence prior to it being entered into the system.

The Criminal Justice Modernisation and Abusive Domestic Behaviour Reviews (Scotland) Bill contains several provisions relevant to the use of digital evidence. For example, section 5A of the Bill as passed provides that where the prosecution uses police body-worn video footage as evidence, any details of time and location recorded on the footage are sufficient evidence of those matters. This would be

subject to the right of the defence to serve notice that it disputes the accuracy of the time and/or location.

UK Ministry of Justice

In relation to England and Wales, in January 2025 the Ministry of Justice issued a call for evidence on the use of evidence generated by software in criminal proceedings. It noted that:

"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."

The call for evidence highlighted concerns arising from the Post Office Horizon scandal, and a legal presumption in England and Wales that computers are operating correctly when producing evidence. An article on the website of the Law Society (of England and Wales) provides some additional background on the call for evidence.

The Post Office's Horizon IT system was piloted from 1996 and rolled out in 2000. Errors in the system wrongly indicated shortfalls in sub-postmasters' accounts. This led to demands for the repayment of sums not actually owed and prosecutions. It affected people in Scotland as well as other parts of the UK. In relation to Scotland, the Post Office (Horizon System) Offences (Scotland) Act 2024 was enacted in response to resulting miscarriages of justice, with relevant convictions being quashed. Similar legislation relating to miscarriages of justice in other parts of the UK was taken forward in the UK Parliament.

In relation to the above-mentioned legal presumption in England and Wales, the COPFS have advised SPICe that:

"There is no legal presumption in Scotland that computer systems are operating correctly when producing evidence. Instead, Scots law, as indicated above, relies upon evidence as to the provenance of the item of evidence before it is in any way evidentially meaningful."

Frazer McCallum

Senior Researcher

5 November 2025

Published by the Scottish Parliament Information Centre (SPICe), an office of the Scottish Parliamentary Corporate Body, The Scottish Parliament, Edinburgh, EH99 1SP

Annexe C: Written submissions

Scottish Government written submission, 30 October 2025

PE2185/A: Introduce stronger safeguards around the use of digital material in court proceedings

Does the Scottish Government consider the specific ask[s] of the petition to be practical or achievable? If not, please explain why.

The Scottish Government does not consider that the action called for by the petition is necessary or practical.

Issues around the gathering and presentation of evidence are matters for Police Scotland and the Crown Office and Procurator Fiscal Service who act independently in the investigation and prosecution of alleged offences.

There exist a number of safeguards and processes to ensure that concerns around the authenticity of any digital evidence can be raised and investigated. That includes disclosure obligations that the Police and Crown are under which ensure that relevant information gathered by the police is reported to prosecutors who in turn will consider and disclose to the defence. The Code of Practice issued under Part VI of the Criminal Justice and Licensing (Scotland) Act 2010 provides guidance in relation to the disclosure of evidence in criminal proceedings.

Where digital material disclosed gives rise to concerns raised in the petition over manipulation or fabrication, as with other types of evidence there are avenues available to the defence to challenge that evidence including raising the purported irregularity with the Crown or the Police who may carry out any investigations considered necessary.

Evidential rules safeguard the fairness of proceedings and mean that the provenance of all productions led in criminal trials, whether physical or digital, requires to be established if those productions are to have any evidential value. Put simply, that means that the party seeking to rely on the production must prove where the production came from, or in other words must prove its ‘source’ as called for by the petition.

How a party does that will vary depending on the type of production and whether there is any dispute over its origin or integrity. Where there is no dispute, the facts of the provenance of the production may be agreed by parties and admitted into evidence through a Joint Minute of Agreement. Where there is a dispute, the party seeking to rely on the production will require to lead witnesses to speak to its provenance – the production does not speak for itself.

For example, where the item is a weapon alleged to have been recovered from a crime scene, it is commonplace for the police officer who seized the item to be called to give evidence to that effect. The defence is entitled to test this evidence and if they take issue with any aspect of it, they can challenge it in cross examination. If they choose to, they may also lead their own evidence to rebut the police officer’s position.

Where the item is in a digital format, the same principle applies and the party wishing to rely on the evidence requires to establish the origin of the material. Using the example of a screenshot as referred to in the petition, that will usually mean the person who took the screenshot and submitted it to the police will be required to give evidence to that effect. That may be in addition to the Crown leading results of forensic analysis of phones or other devices from which the screenshot was captured. The defence are entitled to challenge that evidence including cross examining the witness as to whether the witness had manipulated the screenshot before submitting it to the police. The defence may also lead its own evidence to support their position that the material has been manipulated, including providing alternative screenshots, results of their own forensic analysis or oral evidence of the accused or other witnesses.

It will then be for the fact finder (i.e. judge or jury) to decide what to make of the evidence and how it affects their overall satisfaction that the Crown has discharged its burden of proof to the required standard.

The current evidential requirements therefore already mean that any production has to be adequately sourced, in other words, the facts of a production's provenance have to be agreed or proved, and the defence have ample opportunity to consider and test the evidence led by the Crown to do that, and to lead their own evidence in rebuttal.

It is not necessary to impose restrictions requiring material to be time stamped or independently authenticated before being admissible in evidence as these are matters that can already be properly tested in cases where there are concerns. Given the potential array of digital evidence, it may also not be possible or practical for every type of evidence and rather than excluding that evidence altogether, it is more appropriate for the limitations of that evidence to be tested under existing processes.

The Criminal Procedure (Scotland) Act 1995 creates some specific classes of cases in which facts are to be accepted as proved without the necessity of leading evidence, provided necessary notice has been given to the other party and no objection has been taken. This relates to a number of matters including: reports of identification parades, forensic and autopsy reports; and the time and place of video surveillance recordings. The recent Criminal Justice Modernisation and Abusive Domestic Behaviour Reviews (Scotland) Bill adds to that list the date, time and place of Body Worn Video footage as defined in the Bill.

However, there is no general presumption in relation to the provenance of digital evidence that means that this type of evidence is to be accepted without the party that seeks to rely on it leading evidence to establish where it came from.

Is there any further information the Scottish Government wish to bring to the Committee's attention, which would assist it in considering this petition?

Given the petition relates to matters concerning the investigation and prosecution of crime, the Committee may wish to contact the Chief Constable of Police Scotland as well as the Lord Advocate in her capacity as the head of the prosecution system in Scotland for views on the petition.

Criminal Justice Reform Unit | Criminal Justice Division

Petitioner written submission, 8 November 2025

PE2185/B: Introduce stronger safeguards around the use of digital material in court proceedings

Thank you for taking the time to consider my response.

The Scottish Government response

I must express that the Scottish Government's reply to my petition has missed the heart of the issue I raised. This is not simply a matter of what happens in the courtroom; it is about the long, painful months that innocent people can endure before they ever have a chance to defend themselves.

In my own experience, I spent nine agonising months under the weight of false allegations. During that time, I was subjected to public humiliation, constant fear, and even death threats from strangers who believed the accusations. My accuser was free to spread misinformation online while I was silenced by bail conditions, unable to share my side of the story. I lost my belongings, my reputation was attacked, and I came perilously close to ending my own life because of the unbearable stress.

The point of my petition is simple but crucial: before digital evidence is ever used to drag someone through the court system, it must be thoroughly investigated at the very start. In an age where digital manipulation is easy and evidence can be fabricated in moments, we cannot afford to wait until a trial date to discover the truth.

This is about the police doing their job and making those simple checks that we all know are necessary in this digital age. It is frankly unreasonable that these checks are not already standard procedure, because anyone can edit or fabricate evidence on a smartphone. Law enforcement and judicial authorities are well aware of these risks, and yet there remains no formal safeguard to ensure that such material is properly verified before it is acted upon. My petition simply asks that police thoroughly investigate digital evidence before it ever reaches a courtroom so that no innocent person has to endure what I went through.

I would also like to note that I currently have a police complaint still outstanding since May 2025, in which I have pointed out that a simple investigation by the police would have prevented this entire situation. It has since been demonstrated that false digital evidence was provided to the police, something that would have been detected through proper investigation. The second part of my complaint is that I am asking the authorities to now investigate this and hold the individual responsible to account. Yet as of November, I still have not received an answer.

I urge you to see that this is not about adding unnecessary hurdles, but about protecting innocent lives from being upended by unverified accusations. A simple check at the outset would have spared me and many others months of suffering. I hope you will take this into serious consideration so that no one else has to endure what I went through.

Thank you for your understanding and for addressing the true heart of this petition.

The SPICe briefing

I would like to thank the Scottish Parliament Information Centre (SPICe) for preparing such a clear and balanced briefing to accompany my petition. The paper highlights the key issues surrounding the handling and reliability of digital evidence, and I would like to offer the following short response for clarification and context.

The briefing correctly notes that there is currently no legislative requirement specifying how digital material must be verified prior to its use as evidence. This is the central issue my petition seeks to address. At present, digital evidence can be presented and acted upon long before it has been authenticated, verified, or linked to a verifiable source. This gap in legislation has serious implications for both justice and fairness.

While I welcome the development of the Digital Evidence Sharing Capability (DESC) system, as highlighted in the SPICe paper, it is important to note that DESC is primarily concerned with secure storage and sharing. It does not verify authenticity at the point of upload. In other words, DESC ensures that evidence is handled securely after it has been gathered, but it does not ensure that what is being uploaded is genuine or unaltered in the first place.

Similarly, the Crown Office and Procurator Fiscal Service (COPFS) guidance referenced in the briefing describes a process in which “provenance must be proven before evidence attains evidential status,” and that any disputes can be resolved in court. The problem with this approach is timing. These checks and disputes take place after a person has been charged or brought to trial, meaning that individuals can be subjected to lengthy investigations and restrictions based on unverified or fabricated digital material.

The SPICe briefing also mentions the Criminal Justice Modernisation and Abusive Domestic Behaviour Reviews (Scotland) Bill, which introduces provisions for digital evidence audits. However, as the paper accurately points out, these audits concern data handling and retention, not authentication or verification. They do not prevent false or manipulated evidence from entering the process in the first place.

For these reasons, I respectfully submit that the gap identified by SPICe represents a genuine weakness in the current justice framework. My petition simply asks that this gap be addressed by introducing a clear, preventative safeguard requiring that all digital evidence be verifiably sourced, time-stamped, and authenticated before it can be used in court proceedings or relied upon during investigation.

I would again like to thank SPICe and the Committee for their consideration of this issue. It is my sincere hope that this petition will prompt a wider discussion on how Scotland can lead by example in ensuring the integrity of digital evidence and protecting both victims and the wrongly accused alike.