

Written evidence from Stephen Mason (PPS0001)

Response to the Justice Committee call for evidence regarding private prosecutions and safeguards

Response by Stephen Mason, Barrister

<https://ials.sas.ac.uk/about/about-us/people/stephen-mason>

I offer a response to the Justice Committee call for evidence regarding private prosecutions and safeguards.

I do not have the knowledge or expertise to offer comments relating to private prosecutions. I have decided to offer the brief comments below, based on the following statements (my italics):

1. The Commission's referrals are being made on the basis of an abuse of process argument *concerning issues with the Post Office's Horizon computer system* which may have had an impact on the safety of the convictions.
2. The Post Office Horizon cases are a clear example of a large organisation acting as investigator and prosecutor of alleged crimes in which they were also the victim. There is a real risk that organisations in such circumstances will be faced with a conflict of interest that *could call into question their ability to conduct an objective investigation and prosecution.*

The Chair of the Justice Committee, Sir Bob Neill

Item 1: Evidence in electronic or digital form

A. Computers are presumed to be reliable

In 1997, the Law Commission recommended the repeal of s 69 of the Police and Criminal Evidence Act 1984 and a return to the common law presumption: 'In the absence of evidence to the contrary, the courts will presume that mechanical instruments were in order at the material time.' (*Evidence in Criminal Proceedings: Hearsay and Related Topics* (1997), 13.13). The reasons given by the Law Commission for the introduction of this presumption make it clear that the words 'mechanical instruments' include computers and computer-like devices – even though computers and computer-like devices are not mechanical instruments.

Thus it follows that the writers of software code are presumed to be perfect.

The Law Commission did not provide any empirical evidence to justify this presumption. A judge or the senior judiciary has never questioned the presumption. Once a party uses this presumption against you, it is impossible to argue with a judge that the party invoking it should benefit from it. The presumption exacerbates the disparity in available information and resources, especially when an individual is faced with all the strength and power of a corporation.

Judges accept computers are 'reliable', yet companies that write software code include a contract term in the software licence that clearly states that writers of software code are not perfect. Here is an example:

The Licensee acknowledges that software in general is not error free and agrees that the existence of such errors shall not constitute a breach of this Licence

So, who is correct?

Is it the Law Commission and judges who agree that software is ‘reliable’ (whatever that means – no judge has ever determined what ‘reliability’ is, for which see chapter 6 in *Electronic Evidence* – citation below)?

Or is it the people responsible for writing software code, who explicitly state that software is generally not error free?

Many people may dislike me putting this issue in such a forthright manner, but it seems to me, in researching and writing about this topic in detail since 2010, that the legal profession has collectively failed to be curious about this problem, and failed to take a more measured and objective approach to this matter.

For resources that provide evidence to establish the assertion by the Law Commission in 1997 was not correct then and is not correct now, see:

For a full exposition, see Chapter 6 in Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017), Open Access PDF version in the Humanities Digital Library <http://ials.sas.ac.uk/digital/humanities-digital-library/observing-law-ials-open-book-service-law/electronic-evidence>

Peter Bernard Ladkin, Bev Littlewood, Harold Thimbleby and Martyn Thomas CBE, ‘The Law Commission presumption concerning the dependability of computer evidence’, 17 *Digital Evidence and Electronic Signature Law Review* (2020) 1 – 14
<https://journals.sas.ac.uk/deeslr/article/view/5143>

Peter Bernard Ladkin, ‘Robustness of software’, 17 *Digital Evidence and Electronic Signature Law Review* (2020) 15 – 24
<https://journals.sas.ac.uk/deeslr/article/view/5171>

Paul Marshall, ‘The harm that judges do – misunderstanding computer evidence: Mr Castleton’s story’, 17 *Digital Evidence and Electronic Signature Law Review* (2020) 25 – 48 <https://journals.sas.ac.uk/deeslr/article/view/5172>

B. The failure of the legal profession: education

Why has the legal profession consistently avoided requiring lawyers to learn about this topic?

I was a member of the IT Panel of the Bar of England and Wales 2000-2018. I persuaded my colleagues that this was an essential topic for would-be barristers, and the Panel submitted to those responsible for vocational training that this topic should be on the curriculum, but as far as I am aware, it is still not covered. The suggestion by Capps (below) that it should be post-qualification compulsory continuing professional development is probably the best way to do this, and can be undertaken swiftly.

Resources:

Editorial, 7 *Digital Evidence and Electronic Law Review* (2010), 5-6
<https://journals.sas.ac.uk/deeslr/issue/view/307>

Denise H. Wong, 'Educating for the future: teaching evidence in the technological age', 10 *Digital Evidence and Electronic Law Review* (2013), 16 – 24

Deverall Capps, 'Fitting a quart into a pint pot: the legal curriculum and meeting the requirements of practice', 10 *Digital Evidence and Electronic Law Review* (2013), 23 – 28

<https://journals.sas.ac.uk/deeslr/issue/view/310>

C. Disclosure

Often parties in control of evidence in electronic form object to disclosure because of the resources and cost that this entails.

Let us examine this in detail:

(i) Companies and other businesses use computers and computer-like devices for a number of reasons, but one that stands out is because it is alleged to reduce costs, with the consequence that some of the human work-force can be made redundant, and profit can be increased.

(ii) There is no doubt that in the twenty-first century, it is now a given that computers and computer-like devices are an essential part of running any organization. One consequence is that much evidence about their operations is automatically retained than previously went unrecorded.

(iii) When a dispute or prosecution occurs, the parties have to accept that a vast amount of evidence is, for their own convenience, in electronic form. This must be a factor that each takes into account when deciding what legal action, if any, they take. A judge or members of a jury will not be asked to determine causation in an accident between drivers of motor vehicles merely by looking at the body of each vehicle and reaching a conclusion. It will be expected that relevant evidence about the engine, tyre pressure and braking systems will be considered and adduced as evidence to help determine causation.

Why does an organization that controls evidence in electronic form have some sort of get-out excuse to argue that, because of the cost, relevant evidence in their possession should not be disclosed? This is an odd argument, and one that many judges seem to have accepted.

Electronic records may have to be processed to extract those that are disclosable, which may be a new cost; and they may be held in a form which only the disclosing party's tailor-made software can make accessible to users; and to make that software available may require third-party consent, licensing fees and the training of operators of the recipient party to enable it to be used. This means that the proportionality of the cost to the litigation may become relevant, though it is doubtful whether that is a legitimate consideration in criminal proceedings. An additional point is whether the discloser's claims about the cost be trusted or verified. Who is competent to do this?

The importance of disclosure in relation to the digital world in which we now live is indicated in: Stephen Mason, 'Artificial intelligence: Oh really? And why judges and lawyers are central to the way we live now – but they don't know it', *Computer and Telecommunications Law Review*, 2017, Volume 23, Issue 8, 213 – 225.

Item 2: Conduct an objective investigation and prosecution

This aspect of evidence in electronic form is significant, and affects everybody in the criminal justice system. One example is the prosecution of nurses in the Princess of Wales Hospital in Bridgend, who were indicted on charges relating to alleged falsification of patient notes regarding blood glucose levels. Two nurses entered pleas of not guilty, and a trial ensued. The following is of relevance:

(i) The police and the prosecution lawyers had assumed that the glucometers used to test blood glucose levels, together with the hospital IT systems, were reliable, even though the IT administrators knew the systems required human intervention.

(ii) The police did not question the management of the data, and there was no evidence about the day-to-day management of the data.

(iii) The prosecution also claimed that the devices were accurate as blood glucose meters. This was not relevant. The relevant issue was whether the glucometers reliably transmitted test data to the centralised patient record system (which it did not).

(iv) It did not appear that the police or the prosecution bothered to research this topic – if they had, they would have discovered a number of relevant articles regarding the practical problems of the device and getting the data to the central computer.

The judge concluded that the prosecution evidence was unreliable and was therefore excluded. The prosecution response was to offer no evidence. There the criminal matter ended for the nurses who entered pleas of not guilty – although they were to face continuing problems that have affected their lives since, and continue to do so.

Resources:

For a summary, see *Electronic Evidence*, 9.9-9.95.

Harold Thimbleby, 'Misunderstanding IT: Hospital cybersecurity and IT problems reach the courts', 15 *Digital Evidence and Electronic Law Review* (2018) 11 – 32 <https://journals.sas.ac.uk/deeslr/article/view/4891>

Ruling in *R v Cahill; R v Pugh* 14 October 2014, Crown Court at Cardiff, T20141094 and T20141061 before HHJ Crowther QC, 14 *Digital Evidence and Electronic Signature Law Review* (2017) 67 – 71 <https://journals.sas.ac.uk/deeslr/article/view/2541>

Proposal

It is suggested that consideration be given to providing compulsory informative educational workshops on the topic of electronic evidence for all parties in the criminal justice system, and the topic be a compulsory part of the vocational training of all lawyers.

June 2020