

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htmComputer Law
&
Security Review

Comment

Electronic evidence: A proposal to reform
the presumption of reliability and hearsay[☆]Stephen Mason^{*}

Barrister, specialising in digital evidence and electronic signatures

A B S T R A C T

Keywords:

Electronic evidence
s. 69 Police and Criminal Evidence
Act 1984
Criminal Justice Act 2003

There is a general concern amongst judges, lawyers and legal scholars that evidence in digital format is not to be trusted, given that it can be altered and manipulated with ease. Some jurists have called for a UN Convention on matters relating to the authentication and admissibility of electronic evidence. It is debatable whether such a Convention is necessary, but guidance of an international nature might be welcome, providing that any such guidance remains guidance, and does not ossify into legal requirements that fail to take into account the dynamic and constantly developing changes in information technology. In any event, the accuracy of the presumption in England & Wales that a computer is in order at the material time is highly debatable, and it is suggested that this presumption ought to be reformed.

© 2013 Stephen Mason. Published by Elsevier Ltd. All rights reserved.

In England and Wales, the common law presumption formulated by the Law Commission relating to mechanical instruments was adopted after the repeal of s 69 of the Police and Criminal Evidence Act 1984 in 1999.¹ The presumption included computers by implication (or more accurately, digital data). The Law Commission formulated the presumption as follows: 'In the absence of evidence to the contrary, the courts will presume that mechanical instruments were in order at the material time'.² In criminal proceedings, s 129(2) of the Criminal Justice Act 2003 created a presumption that a mechanical device has been properly set or calibrated:

(a) is made otherwise than by a person, but
(b) depends for its accuracy on information supplied (directly or indirectly) by a person, the representation is not admissible in criminal proceedings as evidence of the fact unless it is proved that the information was accurate.

(2) Subsection (1) does not affect the operation of the presumption that a mechanical device has been properly set or calibrated.

129 Representations other than by a person

(1) Where a representation of any fact—

1. The problem with the presumption

This is a problem that affects all jurisdictions across the globe, and there are varying degrees of concern relating to the

[☆] With thanks to Nicholas Bohm for reviewing this article.

^{*} Associate Research Fellow, Institute of Advanced Legal Studies, Charles Clore House, 17 Russell Square, London WC1B 5DR UK.

E-mail addresses: stephenmason@stephenmason.eu, stephenmason@stephenmason.co.uk.

URL: <http://www.stephenmason.eu>

¹ Section 69 ceased to have any effect by s 60 of the Youth Justice and Criminal Evidence Act 1999, and Schedule 6 also repealed s 69.

² Evidence in Criminal Proceedings: Hearsay and Related Topics (Law Com no 245, 1997), 13.13.

evidence adduced in legal proceedings and how to assess the authenticity of evidence in digital format.³ The problem with the presumption that a computer is deemed to be ‘in order’, or ‘properly set or calibrated’ is that software and the associated systems have become more complex. This means that it has become progressively more challenging to test software to reflect the way the users will use the product. This does not negate the fact that software written by human beings has always been – and continues to be – subject to errors.⁴

The Law Commission commented about the practical issues of challenging the presumption at 13.14:

‘Where a party sought to rely on the presumption, it would not need to lead evidence that the computer was working properly on the occasion in question unless there was evidence that it may not have been – in which case the party would have to prove that it was (beyond reasonable doubt in the case of the prosecution, and on the balance of probabilities in the case of the defence).’

There are problems with judicial comments on this topic.

- (i) First, there is no definition of what is meant by ‘in order’. A computer might be ‘in order’ but not in the way an owner or user expects, because a computer can be both reliable and functioning consistently, yet perform functions without the authority or knowledge of the owner, and a third party can instruct a computer to do things that the owner neither authorises nor is aware of.
- (ii) Second, it will not always be obvious whether the reliability of digital evidence is immediately detectable without recourse to establishing whether the software code is not at fault.

This leads to the logical conclusion articulated by Eric Van Buskirk and Vincent T. Liu⁵

‘The Presumption of Reliability is difficult to rebut. Unless specific evidence is offered to show that the particular code at issue has

³ For books on the topic of electronic evidence, see (in alphabetical order): Stephen Mason, gen ed, *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012) covering Australia, Canada, England & Wales, European Union, Hong Kong, India, Ireland, New Zealand, Scotland, Singapore, South Africa and the United States of America; Stephen Mason, gen ed, *International Electronic Evidence*, (British Institute of International and Comparative Law, 2008) covering Argentina, Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Egypt, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, Netherlands, Norway, Poland, Romania, Russia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Thailand and Turkey; George L. Paul, *Foundations of Digital Evidence* (American Bar Association, 2008) covering the United States of America with some additional chapters; Paul R. Rice, *Electronic Evidence – Law and Practice* (American Bar Association, 2005) covering the United States of America; Daniel M. Scanlan, *Digital Evidence in Criminal Law* (Thomson Reuters Canada Limited, 2011) covering criminal proceedings in Canada, and Allison Stanfield, *Computer Forensics, Electronic Discovery & Electronic Evidence* (LexisNexis Butterworths, 2009) covering Australia.

⁴ As described in detail in *Electronic Evidence*, chapter 5.

⁵ Eric Van Buskirk and Vincent T. Liu, ‘Digital Evidence: Challenging the presumption of reliability’, *Journal of Digital Forensic Practice* 1.1 (2006), 20.

demonstrable defects that are directly relevant to the evidence being offered up for admission, most courts will faithfully maintain the Presumption of Reliability. But because most code is closed source and heavily guarded, a party cannot audit it to review its quality. At the same time, however, source code audits are perhaps the best single way to discover defects.

This difficulty gives rise to an important question: if a party cannot gain access to source code without evidence of a defect, but cannot get evidence of a defect without access to the source code, how is a party to rebut the Presumption? Rather than wrestle with, or even acknowledge, this conundrum, most courts simply presume that all code is reliable without sufficient analysis.’ (Footnotes omitted)

The party contesting the presumption will rarely be in a position to offer substantial evidence to substantiate any challenge, because the party facing the challenge will generally be in full control of the computer or computer systems that are the subject of the challenge, although it is not always the case, given the promotion of cloud computing and recourse to sub-contracting on a significant scale.

2. The current practice in criminal proceedings

Prosecutors adduce electronic evidence in proceedings via s 117 of the Criminal Justice Act 2003, which provides a statutory exception to the hearsay rule for documents created in the course of a trade, business, profession or other occupation. It seems, from the point of view of practice, that defence lawyers in England and Wales regularly agree to the inclusion of electronic evidence under this section on the basis of the presumption. However, the provisions of s 117 do not remove the requirement that the evidential foundations have to establish before the evidence can be admitted. It appears that prosecutors are aware of the position, but defence lawyers do not, in general, appreciate this very important distinction.

Regarding the provisions of s 129(2) of the Criminal Justice Act 2003, the presumption that a mechanical device has been properly set or calibrated arguably refers to devices such as breathalyser devices, not computers or sophisticated networks. The commentary to s 129 does not clarify the position:

‘432. This section provides where a statement generated by a machine is based on information implanted into the machine by a human, the output of the device will only be admissible where it is proved that the information was accurate. Subsection (2) preserves the common law presumption that a mechanical device has been properly set or calibrated.’

Additional confusion arises between the words to describe the presumption by the Law Commission that mechanical instruments were ‘in order at the material time’ and that provided by the explanation, and more crucially the statute, which uses the words ‘properly set or calibrated’.

3. The lack of guidance

There is no authoritative guidance in relation to the meaning of the words ‘reliable’, ‘in order’, ‘accurate’, ‘properly set or

Download English Version:

<https://daneshyari.com/en/article/466753>

Download Persian Version:

<https://daneshyari.com/article/466753>

[Daneshyari.com](https://daneshyari.com)