EDITORIAL

The editors of this journal have the privilege to read and review a number of thought-provoking articles about electronic evidence, from all over the globe. We now live in a world where the use of electronic devices is ubiquitous and electronic information is created, stored, retrieved an exchanged every day; millions of records and documents comprise potential evidence. Although electronic evidence has existed for decades, it has only been in the last twenty-five years that electronic forms of communication and information exchange have become the norm.

This vast array of electronic evidence has led to the legislatures and courts in many jurisdictions to create rules applying to this new paradigm. It has caused us to question whether such rules are adequate, when often they have been developed based on the laws around paper.

One such rule is the presumption that computers are reliable. This presumption is based on the understanding that a computer is made to function properly and produce the result expected of it.

This presumption, developed in the mid to late 1990s, was designed to allow evidence produced by mechanical devices to be admitted into evidence without the need to prove the reliability of the device. Such a presumption makes sense, because it can save considerable court time, and the presumption can always be rebutted if there is evidence to the contrary, that is, the mechanical device is not, in fact, reliable.[1]

The words 'mechanical instruments' include computers and computer-like devices, even though computers and computer-like devices are not mechanical instruments.

A computer is made up of a number of components: the hard drive upon which data is stored, an operating system and application software. It is this complex combination of components that allow a computer to operate, and this can be immediately distinguished from a mechanical device with 'moving parts'. Any of the components within a computer could fail the 'reliability' test. However it is application software that we consider in more detail.

The implication that software code should benefit from the assertion that it forms part of a mechanical instrument and is therefore 'reliable', should be challenged.

Is software code 'reliable'?

Judges often use the word 'reliable' to describe software code in relation to the presumption.[2] No attempt has been made to explain what this means in relation to software in any jurisdiction.

By way of example, the provisions of the Canada Evidence Act (R.S.C., 1985, c. C-5). Section 31.1 provides as follows:

> Any person seeking to admit an electronic document as evidence has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic document is that which it is purported to be.

This is not contentious. The best evidence rule historically applied to all documents, which was replaced by a 'system integrity' requirement. Clause 31.2(1) provides for requiring the 'proof of the integrity of the electronic documents system by or in which the electronic document was recorded or stored'. However, the difficulty lies in the provisions of 31.3(a):

> For the purposes of subsection 31.2(1), in the absence of evidence to the contrary, the integrity of an electronic documents system

[1] In 1997, the Law Commission formulated the common law presumption in the law of England and Wales that '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*, 13.13.

[2] For full details, see Chapter 6 of Stephen Mason and Daniel Seng, editors, *Electronic Evidence* (4th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017), an open source publication.

> by or in which an electronic document is recorded or stored is proven
>
> > (a) by evidence capable of supporting a finding that at all material times the computer system or other similar device used by the electronic documents system was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic document and there are no other reasonable grounds to doubt the integrity of the electronic documents system;

The words 'operating properly' stand out. The presumption remains in Canadian legislation, yet 'operating properly' is not defined,[3] although Walsh J in *Her Majesty the Queen v. Dennis James Oland* 2015 NBQB 245 dealing with a trial within a trial regarding the admission of evidence before trial, noted, at [63]:

> 'I am satisfied on circumstantial evidence that that system was working properly – because it would necessarily be designed and relied upon to accurately record that information given the nature and purposes of that information (i.e. phone usage records kept in the ordinary and usual course of business) and the nature of the business (i.e. by a major communication service provider).'

He also considered, at [72], that the 'system was operating properly given the nature of the resulting information, i.e. it did what was expected of it.' In making these comments, the judge assumed that software code was necessarily designed and relied upon to accurately record data.[4]

This is a circular argument that one does not expect in a court of law if the purpose of a trial is to test the evidence.

A computer is made to function properly and produce the result expected of it

The industry knows that devices controlled by software code generally produce the result expected of it if the software acts in the way the designers anticipate. It does not follow that this is always the case, as indicated in chapter 6 of *Electronic Evidence*. Furthermore, software programmers know their code is not reliable, because every software licence includes a term similar to the following:

> 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

The insistence on the presumption that computers are reliable and simultaneously enforcing contract clauses similar to the model clause noted above creates dissonance and unfairness.

Two significant problems follow from the 'understanding' that a computer is made to function properly and produce the result expected of it. The first is that most devices controlled by software code placed on the device are also controlled by software code stored on other devices and main frames across the globe. This means that any single device interacts with many other devices, thus rendering the 'understanding' false. Most of the software code we interact with today is resident on many other platforms and systems, and no single device can be considered to be functioning properly, and it cannot be considered to be right that a series of devices linked together by software code – such as banking

[3] Judge Castor H.F. Williams refers to 'operating properly' in *R. v. Adams*, 2009 NSPC 15, but does not define what he meant by the term; *R. v. Nardi*, 2012 BCPC 0318, *R. v. Nde Soh*, 2014 NBQB 20 and *R. v. Miro*, 2016 ONSC 4982 for the same point; in a ruling on the admissibility of digital data from Blackberries, Band J found the presumption to operate without defining what it meant in *R. v. Avanes*, 2015 ONCJ 606; Baltman J referred to circumstantial evidence that a computer was operating properly in *R. v. C.L.*, 2017 ONSC 3583.

[4] *Thacker v Iamaw, District Lodge 140*, 2016 CanLII 62600 (BC LA) and 2017 CanLII 79369 (CA LA) where the arbitrator made similar assumptions. Such an assumption is not necessarily warranted, for which see Luciana Duranti and Corinne Rogers, 'Trust in digital records: An increasingly cloudy legal area', *Computer Law and Security Review*, (2012) 28(5), 522 – 531.

systems – ought to benefit from the presumption that computers are reliable.

The difficulty this false presumption causes in legal proceedings

The presumption acts to place an evidential burden on the party opposing the presumption, and if they succeed, the relying party is required to discharge the legal burden in relation to the 'reliability' of the machine, and therefore the authenticity or integrity and the trustworthiness of the evidence. The proponent must prove the authenticity of the evidence before it is admitted and can be relied upon, yet this presumption acts to bypass this requirement.

The problem for the lawyer making the challenge is that they will rarely be in a position to offer evidence to substantiate any challenge. Only the party in possession of the electronic evidence has the ability to understand fully whether the computer or computers from which the evidence was extracted can be trusted.

The presumption asserts something positive. The opposing party is required to prove a negative in the absence of relevant evidence from the program or programs that are relied upon. In criminal proceedings, this has the unfair effect of undermining the presumption of innocence, and in civil proceedings the party challenging the presumption must convince a judge to order up the delivery of the relevant evidence, including software code, if the evidence is to be tested properly.

The proponents of the presumption have never provided any evidence to demonstrate the accuracy of the assertion.

To remedy this imbalance, we suggest a protocol for challenging the authenticity of electronic evidence in criminal proceedings has been suggested:[5]

> **In criminal proceedings**
>
> To require the defence to warn the trial judge in advance that the authenticity of identified aspects of the evidence will be questioned, and to set out the grounds upon which the challenge is made.[6] If this first hurdle is overcome, then it will be for the trial judge to decide whether a trial within a trial is necessary, and if so, to set out the parameters, including the standard of proof, for which a ruling is required. Where the decision is made to hold a trial within a trial, it will be useful for the judge to set out the scope of the hearing.
>
> **In civil proceedings**
>
> To presume the authenticity of the evidence before trial at the disclosure/discovery stage, and for the party challenging the authenticity of identified aspects of the evidence to notify the opposing party and the court in advance of trial.

[5] As suggested in *Electronic Evidence*, 6.168 – 6.174.

[6] To a certain extent this might be already happening, for which see Oriola Sallavaci, 'Streamlined reporting of forensic evidence in England and Wales: Is it the way forward?', (2016) 20(3) E & P 235.

Submissions

The Review seeks and encourages original submissions from judges, lawyers, academics, scientists and technicians; students in relation to postgraduate degree work and versions of dissertations, where the student has passed the relevant course and the dissertation has been marked. The IT industry, certification authorities, registration authorities and suppliers of software and hardware are also encouraged to engage in the debate by submitting articles and items of news.

The length of an article can vary. There is no fixed length. The aim is to publish articles of good quality that adds to the debate and knowledge of readers, discuss recent developments and offer practical advice. All articles will be in English, and contributors are requested to write using shorter, rather than longer sentences, because the audience is international.

Submissions should be sent as an attachment to an e-mail addressed to stephenmason@stephenmason.co.uk or through the online submission options on the journal's homepage at: http://journals.sas.ac.uk/deeslr/.

All papers are peer reviewed blind.

See our **Guide for Authors – submission and editorial information** at: http://ials.sas.ac.uk/digital/ials-open-access-journals/digital-evidence-and-electronic-signature-law-review/digital-1

Copyright, licence and acknowledgement

The contact details of the author should be included in the submission (name, qualifications, name of firm, company or university, full postal address, web address), plus a brief biography demonstrating expertise and experience of up to but no more than 50 words in length.

The author retains copyright and grants the publishers of the Review a licence to publish the article in the Review and to create and maintain digital copies on the internet at the discretion of the publisher and via third parties in subscription databases. The author warrants that they are the owner of all rights of copyright in the article.

Work published in the open access version of **Digital Evidence and Electronic Signature Law Review** on the SAS Open Journals System is licensed under a Creative Commons License. Where the author subsequently publishes the article, the author is requested to acknowledge the article first appeared in the Review, in whatever format it is subsequently published.

Those who contribute items to **Digital Evidence and Electronic Signature Law Review** retain author copyright in their work but are asked to grant two licences:

1. One is a licence to the Institute of Advanced Legal Studies, School of Advanced Study of the University of London, enabling the Institute to reproduce the item in digital form, so that it can be made available for access online in the Open Journals System and repository and website. The terms of the licence, which you are asked to grant to the University for this purpose, are as follows:

> 'I grant to the University of London the irrevocable, non-exclusive royalty-free right to reproduce, distribute, display, and perform this work in any format including electronic formats throughout the world for educational, research, and scientific non-profit uses during the full term of copyright including renewals and extensions'.

2. The other licence is for the benefit of those who wish to make use of items published online in IALS Student Law Review and stored in the e-repository. For this purpose we use a Creative Commons licence allowing others to download your works and share them with others as long as they mention you and link back to your entry in the **Digital Evidence and Electronic Signature Law Review** and/or SAS-SPACE, but they cannot change them in any way or use them commercially.

Where the author subsequently publishes the article, the author is requested to acknowledge the article first appeared in the Review, in whatever format it is subsequently published. The publisher owns the copyright to the text as it appears in the published journal.

The usual rights of editorial control exist with the publisher.