Electronic evidence – some of the problems

Notes to accompany talk

For a webinar with the CEELI Institute, o.p.s

30 June 2020

By

Stephen Mason*

In the context of online hearings, prove the following:

> That you are talking to the correct parties, and not imposters.
>
> Is it a fact you are in touch virtually with the authorized people?
>
> What assumptions are you making in the absence of technical evidence that you are speaking with the correct people?

If you have no knowledge of computer or software, how can you know you are correct?

Introductory observations about understanding electronic evidence

A need to change concepts

> When did it begin?
>
> Arguably by the 1960s for many people, even if they were not aware
>
> Where are we now?
>
> The problem is that some judges, lawyers and legal academics do not understand that:
>
> The basis for understanding evidence has shifted permanently
>
> Their old knowledge is not adequate for dealing with evidence in digital form
>
> You cannot think of paper when considering electronic evidence

The historical viewpoint

> In recent times, information has been stored on paper (China c2nd century AD; Europe c13th century)
>
> Rules around documentary evidence developed in the 18th century
>
> The industrial revolution produced typewriters, carbon paper and filing cabinets, all on paper
>
> The photocopier introduced an easy method of duplicating documents, still on paper
>
> Certain assumptions could be made around paper
>
> Now we have the information revolution: most documents only exist digitally

---

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

Paper and digital

Paper meant the medium and the content were bound together

Digital information is completely different

At its basic level, 'bits and bytes' comprise the content: 0s and 1s

The medium can be many disparate devices

Software written by human beings is required to read and interpret the data (many fail to understand this elementary point)

The rules established for paper no longer apply

The need for a conceptual change

We know about the information revolution: we know that most documents only exist digitally

But electronic evidence has very different characteristics to paper

The normal rules of evidence that have developed with respect to the authentication of (mainly) paper evidence are being applied to electronic evidence

The rules established for paper no longer apply

With its unique characteristics, complex questions about the integrity and security of electronic evidence are raised which must be examined when considering how to authenticate electronic evidence

The concept of original?

For a discussion, see:

Stephen Mason, 'Electronic evidence and the meaning of 'original'', *Amicus Curiae* The Journal of the Society for Advanced Legal Studies, Issue 79, Autumn 2009, 26 – 28

Available as a free download from: http://sas-space.sas.ac.uk/2565/

All digital data is a copy of a copy of a copy …..

What, perhaps, we need to think about is 'first-in-time' evidence

Characteristics of electronic evidence

The dependency on machinery and software

The mediation of technology

Speed of change

Volume and replication

Metadata

Storage media

Illicitly obtaining confidential data

Anti-forensics and the interpretation of evidence

Destruction of data; falsifying data; hiding data; attacks against computer forensics; trail obfuscation

Sources of electronic evidence

Physical devices

Computers; mobile telephones; smartphones; PDAs; tablets; etc.

The components

Hardware; the processor; storage; software (system software; application software); the clock; time stamps; storage media and memory; data formats; powering up and powering down

Networks (e.g. internet; the cloud; corporate intranets; wireless networking; cellular networks; dial-up)

Applications (e.g. e-mail; instant messaging; computer to computer; social networking)

Definitions

Burkhard Schafer and Stephen Mason, in 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)

Paragraph 2.6:

'Electronic evidence: data (comprising the output of analogue devices or data in digital form) that is manipulated, stored or communicated by any manufactured device, computer or computer system or transmitted over a communication system, that has the potential to make the factual account of either party more probable or less probable than it would be without the evidence.'

The *European Informatics Data Exchange Framework for Court and Evidence* project identified a significant number of definitions http://www.evidenceproject.eu

In particular, see 'D3.1 Overview of existing legal framework in the EU Member States (Deliverable prepared by Partner 2 – RUG)

Other issues (this list is not exhaustive)

Principles of handling digital evidence; guidelines

Investigation (+ international context)

Search and seizure (+ international context)

Challenges of international investigations (evidence in the cloud, admissibility)

Some trial considerations (authenticity; methods of presentation)

Examination, analysis, interpretation and reporting

Methods; tools (scientific reliability); qualifications of the investigator

Encryption (protected data)

Authenticity

Proof of intent

Free materials

Council of Europe on digital evidence
https://www.coe.int/en/web/cdcj/activities/digital-evidence

Draft Convention on Electronic Evidence
https://journals.sas.ac.uk/deeslr/article/view/2321

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)

ISBN 978-1-911507-05-5 (hardback edition)

ISBN 978-1-911507-09-3 (paperback edition)

ISBN 978-1-911507-08-6 (epub version)

ISBN 978-1-911507-07-9 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

Digital Evidence and Electronic Signature Law Review:
https://journals.sas.ac.uk/index.php/deeslr

The *Digital Evidence and Electronic Signature Law Review* has published a significant number of articles about the law and digital forensics, and also provides Book Reports in most years with reports of relevant books, and also lists those haven taken or are taking PhDs in associated topics. A cumulative index is published every five years.

Software failures (See Chapter 6 in *Electronic Evidence* for more examples)

Aviation

Errors in aviation software can have disastrous, or near disastrous, consequences. It can be caused by something as simple as bad coding. By way of example, consider the F-22A Raptor advanced tactical fighter, which entered service with the US Air Force in 2005. In February 2007, 12 of these aircraft were flying from Hickham AFB in Hawaii to Kadena AB on Okinawa. All of the aircraft experienced simultaneous and total software failure with their navigational console when their longitude shifted from 180 degrees West to 180 East. The jets were accompanied by tanker planes, which meant the pilots in the tankers were able to guide the jets back to Hawaii.

Lewis Page, 'US Superfighter software glitch fixed', *The Register*, 28 February 2007

https://www.theregister.co.uk/2007/02/28/f22s_working_again/

Motor vehicles

Volkswagen AG, Audi AG, and Volkswagen Group of America, Inc taken to task regarding four-cylinder Volkswagen and Audi diesel cars covering years 2009-2015 that included software that circumvents the emissions standards for some air pollutants.

https://www.epa.gov/vw/learn-about-volkswagen-violations

Banking

A coding error caused Deutsche to reverse the buy/sell indicator for its CFD Equity Swaps in 2013. This meant it reported them inaccurately to the Financial Conduct Authority (FCA). The FCA imposed a financial penalty of £4,7818,800 on Deutsche for failing to provide accurate reports in accordance with the provisions of the Markets in Financial Instruments Directive.

https://www.fca.org.uk/publication/final-notices/deutsche-bank-ag-2015.pdf

Examples of the decisions of judges

For a very poor ATM banking decision in which it was clear that the judges accepted the claimant was lying (they did not say this explicitly) and therefore the technical evidence submitted was correct (they were looking a the wrong problem), see:

> 5 October 2004, XI ZR 210/03, published BGHZ 160, 308-321 Bundesgerichtshof (Federal Court of Justice), commentary by Dr Martin Eßer, further commentary by Dr Thomas Kritter
>
> *Electronic signature (PIN); ATM; card holder; theft of card; subsequently used by thief; liability*
>
> 6 *Digital Evidence and Electronic Signature Law Review* (2009), 248 – 254
>
> https://journals.sas.ac.uk/deeslr/issue/view/306

Compare the decision of the Federal Court of Justice to the much better decision by the Supreme Court of Lithuania, which set out the types of evidence a court should expect to see by a bank:

> Ž.Š. v Lietuvos taupomasis bankas, Civil case No. 3K-3-390/2002, Supreme Court of Lithuania, by Sergejs Trofimovs
>
> *ATM; electronic signature (PIN); liability of the bank*
>
> 6 *Digital Evidence and Electronic Signature Law Review* (2009), 255 – 262
>
> https://journals.sas.ac.uk/deeslr/issue/view/306

For judicial assumptions that are not warranted, see the following case from Norway:

> Journal number 04-016794TVI-TRON, *Bernt Petter Jørgensen v DnB NOR Bank ASA by the Chairman of the Board* (Trondheim District Court, 24 September 2004)
>
> *Bank card; theft of card; unauthorized use; PIN; electronic signature; burden of proof; liability; gross negligence*
>
> 9 *Digital Evidence and Electronic Signature Law Review* (2012), 117 – 123
>
> https://journals.sas.ac.uk/deeslr/issue/view/309

This case is discussed in:

> Maryke Silalahi Nuth, Unauthorized use of bank cards with or without the PIN: a lost case for the customer?, 9 *Digital Evidence and Electronic Signature Law Review* (2012) 95 – 101
>
> https://journals.sas.ac.uk/deeslr/issue/view/309

Significant scandal in the UK: the Post Office Horizon scandal

For background, see *Electronic Evidence*, 6.143; 7.153 and the following articles (in England & Wales, there is a presumption that computers are reliable – which is the topic of chapter 6 of *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

Stephen Mason, General editor, *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 https://www.biicl.org/books/international-electronic-evidence

An article about the use of cameras in courts that is of tangential interest

Stephen Mason, 'Cameras in the courts: why the prohibition occurred in the UK', *Amicus Curiae The Journal of the Society for Advanced Legal Studies*, Issue 91, Autumn 2012, 22 – 27 https://journals.sas.ac.uk/amicus/article/view/2095

The *Digital Evidence and Electronic Signature Law Review* has published a number of case translations into English from the following jurisdictions: Austria, Belgium, Bulgaria, China, Denmark, Dubai, Estonia, France, Germany, Greece, Hungary, Italy, Japan, Latvia, Lithuania, Mexico, The Netherlands, Norway, Poland, Romania, Spain, Sweden and Turkey.

Forthcoming

In 2020, we will be including the translation of a criminal case from Switzerland of a driver of a Tesla who was convicted of failing to be in control of his vehicle when he put the car into 'automatic' mode and the software crashed it into a stationery object.

For a list of cases translated, see the 2004-2018 cumulative index, see https://journals.sas.ac.uk/deeslr/article/view/4918

Stephen Mason and Professor Daniel Seng are writing an article entitled 'Artificial Intelligence and Evidence' to be published in a Special Issue of the Singapore Academy of Law Journal: https://journalsonline.academypublishing.org.sg/Journals/Singapore-Academy-of-Law-Journal