Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Online Meeting and Lecture

"e-" Changes Everything: A Concise Introduction into Electronic Evidence

Онлайн-встреча и лекция

“e-" меняет всё. Краткое введение в электронные доказательства

Stephen Mason, Barrister and Associate Research Fellow at the Institute of Advanced Legal Studies, School of Advanced Study, University of London

22 December, 2021

IALS INSTITUTE OF ADVANCED LEGAL STUDIES | SCHOOL OF ADVANCED STUDY UNIVERSITY OF LONDON

Outline of talk

General introduction

Authentication

Integrity of evidence

Questions

The need for a conceptual change

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

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:

> "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 we need to think about is 'first-in-time' evidence

Definition

Definition in *Electronic Evidence and Electronic Signatures*, paragraph 1.113:

> '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)'

Some challenges

A claim that the records were altered, manipulated or damaged between the time they were created and the time they appear in court as evidence

The reliability of the computer program that generated the record may be questioned

The identity of the author may be in dispute, or the person that used a mobile telephone

The evidence from a social networking website (for instance) might be questioned as to its reliability

Whether the person alleged to have used their PIN, password or clicked the ‘I accept’ icon was the person that actually carried out the action

Authentication

On authentication generally, see Chapter 6 ‘Authenticating electronic evidence’ in *Electronic Evidence and Electronic Signatures*

It may be necessary to lay down the evidential foundations of digital evidence before the evidence is accepted in legal proceedings

Or

The authenticity of digital evidence may be the subject of a challenge

Trustworthy

The term ‘trustworthiness’ is often used to describe that a thing deserves, or is entitled to, trust or confidence

There are two qualitative dimensions to the concept of trustworthiness:

> Reliability: to demonstrate that the record is capable of standing for the facts to which it attests
>
> Authenticity: the record is what it claims to be

The term ‘authentic’ is used to describe whether a document or data are genuine, or that the document (in the case of digital data) matches the claims made about it

Testing for authenticity

The tests will vary, depending on the source of the data and the type of the data

Consideration should be given to:

- procedures, process and technical measures such as audit logs, system security, and the use of digital signatures – these are all highly relevant in providing for the authenticity of digital data

And

- the methods by which people are required to interact with computers and computer systems

The means of authentication might depend on the source of the data (e.g. computer; smartphone; internet; e-mail, etc.)

Example 1: simple electronic evidence

Web site from France:

Tribunal de grande instance de Mulhouse 1ère chambre civile Jugement du 7 février 2007, Groupe Philippe Bosc v MMT

> (Tim Van Canneyt and Christophe Verdure, 'Bailiffs on the internet and the validity of their certified reports: Lessons learned from the French and Belgian courts', 7 *Digital Evidence and Electronic Signature Law Review*, (2010) 71 – 76)

Example 2: simple electronic evidence

R v Mawji (Rizwan) [For more details of this case, see paragraph 6.123 in *Electronic Evidence and Electronic Signatures*]

The appellant was convicted of making a threat to kill, and part of the evidence included an e-mail sent to the victim dated 31 July 2002, which read:

> 'Hi Bitch,
>
> Don't think you're safe in the UK. I'm going to kill you.
>
> I will make sure I get my hands on you … waiting for you.
>
> Your loving husband.
>
> Riz.'

Rizwan continued

At the trial, a witness for the defence gave evidence:

> (i) to demonstrate how relatively easy it was to produce a document that claimed to be an e-mail, but
>
> (ii) which had nothing to do with the e-mail account from which it purported to come

The defence suggested that somebody else was responsible for sending the e-mail in question

Rizwan: Appeal

In one ground of appeal, the appellant argued that it was necessary to provide evidence of the audit trail or some other similar evidence to show the authenticity of the document

The members of the Court of Appeal rejected this submission

Rizwan: Court of Appeal reasoning

The e-mail did not have to be authenticated in the way suggested by the appellant because of the circumstances surrounding the events and the other evidence in the case

The content of the e-mail was similar to other evidence produced at trial

This went to show that the e-mail was written and sent by the appellant

The finder of fact had to consider whether, in all the circumstances, it was possible that somebody else might have produced the e-mail

The content of the e-mail demonstrated its authenticity on the face of the totality of the evidence

If the e-mail was fabricated, it had to be questioned as to why somebody would go to the length of forging the content of an e-mail that was so obviously linked to the other evidence produced at trial

Integrity of the data

Questions to consider

What confidence can we have that the evidence accurately represents the facts that they are purported to represent?

This leads to:

1. Was there a trustworthy source of information that accurately reflected the facts?

2. If there was, is the evidence presented in legal proceedings generated without error from that source of information?

3. If it was, has the integrity of the evidence been preserved throughout between the time the data was collected to the moment it is relied on in legal proceedings?

Towards an understanding of authentication

The range of considerations to be taken into account will differ, according to:

- the nature of the evidence to be authenticated
- where the evidence is to be found
- local rules of evidence

The means of authentication depends on the individual rules of the jurisdiction

In the majority of cases, oral and circumstantial evidence will be sufficient for most digital data

Complex electronic evidence

See the practical two-phase approach in *Electronic Evidence and Electronic Signatures*, paragraph 5.264 (taken from Marshall and others, 'Recommendations for the probity of computer evidence' 18 *Digital Evidence and Electronic Signature Law Review* (2021) 18 – 26)

https://journals.sas.ac.uk/index.php/deeslr

See also the tests in article 4 of the Draft Convention on Electronic Evidence

Published in Volume 13 (2016) of the *Digital Evidence and Electronic Signature Law Review* as a supplement, S1 – S11

http://journals.sas.ac.uk/deeslr/issue/view/336/showToc

Integrity of evidence

One issue is whether the integrity of the evidence has been preserved between the time the data was collected, to the moment it is relied on in legal proceedings

A hash function is used by digital evidence professionals to prevent the evidence from changing

Estonia – use of the MD5 hash: TlnRnKo 09.01.2017, 1-15-9051

16 *Digital Evidence and Electronic Signature Law* (2019) 71 – 89

China – use of blockchain: *Hangzhou Huatai Yimei Culture Media Co., Ltd. v. Shenzhen Daotong Technology Development Co., Ltd.* (2018) Zhe 0192 Civil Case, First Court No. 81

16 *Digital Evidence and Electronic Signature Law* (2019) 61 – 70

Topics not discussed

Jurisdiction

(for which see the Belgian *Yahoo* case – next slide for links); cloud computing

Admissibility

Sources of electronic evidence

Software and logic (e.g. software as the witness)

Encrypted data

Proof and investigation. This includes, but it not limited to the following:

The process

Practical problems

Good practice

Tools for investigation

Scientific reliability

Competence of witnesses

English translations of every Belgian Yahoo case

Corr. Dendermonde 2 maart 2009, onuitg. (Rechtbank van Eerste Aanleg te Dendermonde (The Court of First Instance in Dendermonde)), by Johan Vandendriessche, *Digital Evidence and Electronic Signature Law Review* 8 (2011) 196 – 207 http://journals.sas.ac.uk/deeslr/article/view/1976/1913

Gent 30 juni 2010, onuitg. (Hof van Beroep (The Court of Appeal in Ghent, third chamber, sitting in criminal matters)), by Johan Vandendriessche, *Digital Evidence and Electronic Signature Law Review* 8 (2011) 208 – 215 http://journals.sas.ac.uk/deeslr/article/view/1977/1914

Cass. 18 januari 2011, nr. P.10.1347.N (Hof van Cassatie (Court of Cassation of Belgium)), by John Vandendriessche, *Digital Evidence and Electronic Signature Law Review* 8 (2011) 216 – 218 http://journals.sas.ac.uk/deeslr/article/view/1978/1915

Brussel 12 oktober 2011, onuitg, Hof van Beroep te Brussel (The Court of Appeal in Brussels, thirteenth chamber, sitting in criminal matters), by Johan Vandendriessche, *Digital Evidence and Electronic Signature Law Review* 9 (2012) 102 – 105 http://journals.sas.ac.uk/deeslr/article/view/2000/1937

P. 11.1906.N/1, commentary by Johan Vandendriessche, *Digital Evidence and Electronic Signature Law Review* 10 (2013) 155 – 157 http://journals.sas.ac.uk/deeslr/article/view/2036/1973

Antwerpen 20 november 2013, 2012/CO/1054 Yahoo! Inc., translated by Johan Vandendriessche, *Digital Evidence and Electronic Signature Law Review* 11 (2014) 137 – 143 http://journals.sas.ac.uk/deeslr/article/view/2138/2068

Nr. P.13.2082.N, 1 December 2015, translated by Johan Vandendriessche, *Digital Evidence and Electronic Signature Law Review* 13 (2016) 156 – 158 http://journals.sas.ac.uk/deeslr/article/view/2310

Questions

Thank you – Спасибо

Free materials

Council of Europe on digital evidence

> *Electronic evidence in civil and administrative proceedings Guidelines and explanatory memorandum*, as proposed by the European Committee on Legal Co-operation (30 January 2019)
>
> Stephen Mason, assisted by Uwe Rasmussen, *The use of electronic evidence in civil and administrative law proceedings and its effects on the rules of evidence and modes of proof* (European Committee on Legal Co-operation, CDCJ(2015)14 final, Strasbourg, 27 July 2016)
>
> https://www.coe.int/en/web/cdcj/activities/digital-evidence

Digital Evidence and Electronic Signature Law Review

> https://journals.sas.ac.uk/index.php/deeslr

Draft Convention on Electronic Evidence

> http://journals.sas.ac.uk/deeslr/issue/view/336/showToc

Further free materials

Open source practitioner book

Stephen Mason and Daniel Seng, editors, *Electronic Evidence and Electronic Signatures* (5th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2021)

Available as open access, hardback, paperback and e-pub:

https://humanities-digital-library.org/index.php/hdl/catalog/book/electronic-evidence-and-electronic-signatures

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

Stephen Mason, editor, *International Electronic Evidence* (British Institute of International and Comparative Law, 2008)

> This text covers the following jurisdictions:
>
> 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