

News Release
London, Wednesday, November 23, 2016

**Announcing the *Draft Convention on Electronic Evidence*.
Published in the UK, the Draft Convention is the first ever treaty dealing
with the status, examination, recognition, and admissibility of electronic
evidence.**

The *Draft Convention on Electronic Evidence* is now published as a supplement to the **Volume 13: 2016** issue of the **Digital Evidence and Electronic Signature Law Review**.

This Draft Convention is the first treaty dealing with the status of electronic evidence, covering civil and criminal proceedings; the investigation and examination of electronic evidence, and general provisions regarding the recognition and admissibility of electronic evidence from foreign jurisdictions.

The Draft Convention was initiated and developed during the summer of 2016 by **Stephen Mason**, Barrister and Author, with authoritative input and contribution from a wide range of legal and technology academics, practitioners and professional worldwide, in litigation and prosecution practice, computer law, data forensics, cybersecurity and evidential reliability.

Dr Stephen Castell, independent international ICT consultant and expert witness, and a NEWA-listed professional, who was one such leading contributor, comments: “This private initiative is long overdue and at last deals with the important area of the intersection of the law and technology relating to professional practices of data forensic investigations and the proper investigation, preservation and presentation of reliable electronic evidence, for both criminal and civil cases”.

The **Draft Convention** is published for consultation with and freely available to all interested and concerned legal and technological investigators, professionals and practitioners, globally. **Stephen Mason**, its author, says: “Please join in to improve the document”.

To obtain and review the *Draft Convention on Electronic Evidence*:

1. Go to <http://journals.sas.ac.uk/deeslr/issue/view/336/showToc>
2. See ‘Documents Supplement’ at foot of contents; click on ‘Draft Convention on Electronic Evidence’ to see Abstract: <http://dx.doi.org/10.14296/deeslr.v13i0.2321>
3. Then click on ‘PDF’ (<http://journals.sas.ac.uk/deeslr/article/view/2321/2245>) to download the full text of the Draft Convention.

Background

Stephen Mason (<http://www.stephenmason.eu/>) is a barrister, called to the Bar by the Honourable Society of the Middle Temple in November 1988. BA (Hons) (History and Educational Philosophy), MA, LL.M., PGCE (FE). Stephen is the recognised authority on electronic signatures and digital evidence, and has assisted many governments, for example in China, the Middle-East, Central America, and businesses in continental Europe and Africa, including the Corporation of London, the Ministry of Justice of the United Arab Emirates, and the government of Trinidad and Tobago.

Some examples of Stephen Mason's recent work:

Council of Europe: Stephen undertook a comparative study and of existing national legal provisions that have been adopted or adapted on the effect of electronic evidence on the rules of evidence and modes of proof, the final report being presented to the 90th plenary meeting of the European Committee on Legal Co-operation in Strasbourg on 28 October 2014.

Commonwealth Secretariat: Work on the International Cooperation Programme regarding the Interception of Telecommunications in the Harare Scheme and the Commonwealth Draft Model Legislation, developing a framework for the interception of telecommunications.

UK Home Office: Member of the Expert Panel on Digital Signatures in the Acquisition of Communications Data within the Criminal Justice System.

Stephen Mason regularly advises on:

- (i) standardisation of technologies and authentication and identification methods;
- (ii) legally enforceable digital signature programmes in global commerce;
- (iii) the factors affecting the use and acceptance of e-signatures in commerce;
- (iv) admissibility of digital evidence internationally;
- (v) specialist e-commerce due diligence in a take-over involving a payment gateway.

Dr Stephen Castell CITP is Chairman of *CASTELL Consulting*, and has for over twenty-five years acted internationally as an expert witness in major complex computer software and systems disputes and litigation, including the largest and longest such actions to have reached the English High Court, and Sydney Supreme Court (<http://www.castellconsulting.com/>).

Twenty years ago Dr Castell pointed out that 'open' Von Neumann computer architecture – now, as then, still the basis for software design and construction of all commercial ICT devices and systems – was inherently insecure (See '*A computer of the simplest kind*', Computer Law and Security Report 10, May-June 1994). Five years before that, Dr Castell authored the *APPEAL Report*, May 1990, a major study commissioned by the CCTA (H M Treasury), on admissibility of computer evidence in court and the legal reliability/security of IT systems, still seen by many practitioners as a definitive study in the field. This concluded with what became known as *Castell's Dictum*: "*You cannot secure an ontologically unreliable technology by use of an ontologically unreliable technology*".

Electronic Evidence has been acknowledged to be based on the concept of a transactional *chain of trust*. Dr Castell identified as far back as 1993 the latter's dependency on *Trusted Third Party Services* ('TTPs'):

"As described by Castell, '*A Trusted Third Party is an impartial organization delivering business confidence, through commercial and technical security features, to an electronic transaction. It supplies technically and legally reliable means of carrying out, facilitating, producing independent evidence about and/or arbitrating on an electronic transaction. Its services are provided and underwritten by technical, legal, financial and/or structural means*' [10]. TTPs are provided and underwritten not only by technical, but also by legal, financial, and structural means [10,11]. TTPs are operationally connected through chains of trust (usually called certificate paths) in order to provide a web of trust...

[10] S. Castell, Code of practice and management guidelines for trusted third party services, INFOSEC Project Report S2101/02, 1993.

[11] Commission of the European Community. Green paper on the security of information systems, ver. 4.2.1, 1994. ..."

In *Security Issues On Cloud Computing*. Pratibha Tripathi, Mohammad Suaib;
Department of Computer Science and Engineering, Integral University, Lucknow, Uttar Pradesh, India.

International Journal of Engineering Technology, Management and Applied Sciences

<http://www.ijetmas.com/> November 2014, Volume 2 Issue 6, ISSN 2349-44761.

Available from: https://www.researchgate.net/publication/272945014_Security_Issues_On_Cloud_Computing

Further Details From

Stephen Mason

Chambers of Stephen Mason
19a Church Street
Langford
BIGGLESWADE
Bedfordshire SG18 9QT
United Kingdom
Telephone: +44 1462 701 036
Email: stephenmason@stephenmason.eu
<http://www.stephenmason.eu/>

Dr Stephen Castell CITP CPhys AFIMA MEWI MIoD

Chairman, CASTELL Consulting
PO Box 334, Witham, Essex CM8 3LP
United Kingdom
Telephone: +44 1621 891 776 Mobile: +44 7831 349 162
Email: stephen@castellconsulting.com
<http://www.CastellConsulting.com>
<http://www.e-expertwitness.com>

David Haley

National Expert Witness Agency (NEWA)
17, The Causeway
Burwell, Cambridge CB25 ODU
United Kingdom
Telephone: +44 1638 601 110
Email: info@newa.expert
<https://www.newa.expert/>

23 November 2016