The concept of a Convention on Electronic Evidence

by Stephen Mason

INTRODUCTION

I have undertaken a great deal of training of judges and lawyers in electronic evidence across the world (India, Tanzania, Thailand, Tonga, United Arab Emirates), and with the Academy of European Law in Europe (Bulgaria, Cyprus, Czech Republic, England, Estonia, France, Germany, Italy, Latvia, Norway, Portugal, Romania, Spain, Turkey, Ukraine). More recently, participants have asked if the United Nations or the Council of Europe were considering a Convention on Electronic Evidence. I am not aware that either body is considering such a Convention. This could be because at the political level there is no interest, and possibly because such a Convention might take some years to develop to the satisfaction of all the parties.

I appreciate that drafting such a Convention at international level between governments needs to include political considerations, and do not wish to make light of this aspect of negotiations, because it is important. However, given that we now live in a networked world, and people do horrible things online, I think it is important to encourage politicians and commercial legal entities to understand that the flow of electronic evidence, especially between prosecutors across legal boundaries, is important for a number of reasons: the successful prosecution of people that have done something seriously wrong and where they have caused loss, harm and distress to innocent victims, and for the social stability of nation states.

In the absence of a discussion of the development of such a Convention at an international level, I concluded that it might be useful to develop such a Convention with the help of judges, lawyers and other interested individuals across the world. I appreciate this is a private initiative, but sometimes private initiatives help. Below is the final version, as jointly published in the *Digital Evidence and Electronic Signature Law Review* and *Amicus*.

DRAFT CONVENTION ON ELECTRONIC EVIDENCE

Summary

The 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.

Convention on Electronic Evidence

London,

Preamble

[The States signatory hereto],

Considering that the aim of the Drafting Committee is to encourage judges and lawyers to appreciate the concept of evidence in electronic form;

Recognising the value of promoting international co-operation with [the other States that are Parties] to this Convention;

Convinced of the need to pursue, as a matter of priority, a common policy on electronic evidence;

Conscious that the profound changes brought about by the machine and software code (collectively "digital systems") have altered the means by which evidence is authenticated, in that the medium and the content are no longer bound together as with paper, and that the rules established for paper do not always apply to evidence in electronic form;

Concerned by the risk that electronic evidence can be misunderstood and misinterpreted;

Recognising that evidence in electronic form has unique characteristics that are significantly different to paper and other objects, which raise complex questions about the integrity and reliability of data in electronic form;

Recognising the need to facilitate the co-operation between States for the proper receipt, handling and authentication of electronic evidence;

Believing that it is in the interests of justice to provide for fairness in legal proceedings;

Have agreed as follows:

Part I – Use of terms

Article 1 – Definitions

For the purposes of this Convention:

"adjudicator" means any person that is lawfully appointed as a judge, arbitrator or to any other role that requires the holder of the office to act in a judicious and unbiased manner;

"attribution" means the assigning of responsibility for or tracing the origin of an act purported to have been performed or committed using or through a computer device, system or network;

"authentication" means the process by which any electronic record, document, statement or other thing is proven to be what it claims to be;

"computer" means any device capable of performing mathematical or logical instructions;

"court" means any international court, national court, statutory arbitral or other tribunal, board or commission according to national law of the contracting state;

"electronic evidence" means evidence derived from data contained in or produced by any device the functioning of which depends on a software program or from data stored on or communicated over a computer system or network;

"electronic record" means data that is recorded or stored on any medium in or by a device programmed by software code and that can be read or perceived by a person or any such device, and includes a display, printout or other output that represents the data;

"device" means any apparatus or tool operating alone or connected to other apparatus or tools, that processes information or data in electronic form;

"digital" means anything that relies on technology based on a binary system or any future development or replacement technology of the same;

"digital evidence practitioner" means a person who is appropriately qualified, and where the law requires, authorised, to investigate and examine evidence in electronic form;

"legal proceeding" means any formal procedure that takes place before any court, national or international, a statutory arbitral or other tribunal, board or commission according to national law and charged with legally defined duties and obligations, or any other formal legal process;

"metadata" means data that describe other data;

"program" means any set of instructions stored in a machine-readable format that can be used to perform a function in a repeatable and reproducible manner;

"relevant legal proceedings" means the legal proceedings for which data in electronic form is requested under a Mutual Legal Assistance Treaty or any other bilateral or multilateral instrument;

"tool" means any device or software program that can be used to identify, secure, examine and analyse electronic evidence.

Part II – Status of electronic evidence

Article 2 – Admissibility of electronic evidence

1. Evidence in electronic form shall be admitted into legal proceedings.

2. Article 2(1) does not modify any existing national rule that applies to the admissibility of evidence, except in relation to the rules relating to authenticity and best evidence.

Article 3 – Agreement on the admissibility of electronic evidence

1. Unless otherwise provided in any law operating in the relevant jurisdiction, an electronic record or document may be tendered, subject to the discretion and rules of the court, if the Parties to the proceedings have expressly agreed to its introduction.

2. Notwithstanding the provisions of Article 3(1), an agreement between the Parties on the admissibility of an electronic record or document does not render the record admissible in a criminal proceeding if at the time the agreement was made

    (a) the accused person or any of the persons accused in the proceeding was not represented by a lawyer;

    (b) except where the adjudicator finds that admitting the record or document into evidence does not prejudice the case for the accused.

Article 4 – Authentication of electronic evidence

1. The party seeking to introduce electronic evidence in any legal proceeding has the burden of proving it is what it claims to be.

2. The matters set out below are to be considered when assessing that evidence in electronic form is what it claims to be:

   (a) The data (both the content and associated metadata) relied upon in any legal proceedings can be shown to be an accurate representation of the prevailing and existing state of those data at the time relevant to the legal proceedings.

   (b) If the data have changed from the moment they were identified (and possibly seized) as potential evidence in legal proceedings, there is an accurate and reliable method of documenting any such changes, including the reasons for any such modifications.

   (c) The continuity of the data between the moment in time the data were obtained for legal purposes and their submission as an exhibit in legal proceedings can be demonstrated.

   (d) Any techniques that were used to obtain, secure and process the data can be tested and shown to have been appropriate for the purpose for which they were applied.

   (e) The technical and organizational evidence demonstrates that the integrity of the data is trustworthy, and can therefore be considered reliable and complete (insofar as the data can be complete), which in turn will depend on the circumstances surrounding the data at the time they were identified as being potentially relevant in legal proceedings.

Article 5 – Best evidence

1. In any legal proceeding, where any printout, document or other physical manifestation of the result or output or appearance of any electronic process, record or any other representation of that process or record has been manifestly or consistently acted on, relied upon, or used as the record of the information represented by or stored on the printout, the printout or other physical manifestation shall be considered the best evidence and admitted as evidence subject to satisfactory proof of its integrity.

2. Where the output of a process is relied upon, and it remains in electronic form, the best evidence rule remains, subject to the provisions of Article 4(2).

3. Article 5(1) and (2) do not modify any domestic rule that applies to the admission of evidence.

Part III – Investigation and examination of digital evidence

Article 6 – Digital evidence practitioner

1. Since digital evidence practitioners are required to make informed judgements about the appropriateness of the tools and techniques they use to secure and preserve electronic evidence, the Parties shall establish minimum standards for their formal education and training.

2. A digital evidence practitioner must be able to provide, in compliance with the necessary court and legal requirements:

   (a) an analysis of their findings, setting out the scientifically agreed basis upon which their judgement is based; and

   (b) shall identify and explain any data that appear to be inconsistent with their findings.

3. The primary duty of the digital evidence practitioner is to the court.

Article 7 – The use of good practice guidelines for electronic evidence

1. The Parties to the Convention shall establish a Forum for the development of good practice and guidelines in the acquisition, handling and otherwise processing of electronic evidence in the form of a set of agreed common requirements.

2. The forum shall:

   (a) Include participation from at least two thirds of all Parties to the Convention.

   (b) Establish its own rules of procedure and may establish subcommittees to consider specific issues.

   (c) Be funded on a basis to be agreed.

   (d) Submit the first edition of its agreed common requirements to the Parties within two (2) years of this Convention coming into force for subsequent adoption by the Parties.

   (e) Produce updates and amendments to the agreed common requirements as deemed desirable and necessary by the Forum and in any case every two years, or a statement that an update is not currently necessary.

3. Except where incompatible or inconsistent with national legislation, codes or procedure, the Parties to this Convention shall implement agreed common requirements on the acquisition, obtaining, packaging, processing and examination of electronic evidence.

4. The agreed common requirements shall be:

   (a) Drafted by reference to the guidelines established by the Forum.

   (b) Adopted within [*time period to be agreed*] of accession to this Convention or within [*time period to be agreed*] of the publication of the first version of the agreed common requirements by the Forum, wherever is the sooner.

   (c) Implemented by all national and government departments charged with legal duties and obligations involving the use, handling or processing of electronic evidence.

5. Any authority responsible for investigating a matter involving the criminal law shall apply and follow the agreed common requirements unless there are exceptional or extenuating circumstances where they cannot be followed.

6. Where, under Article 7(5) above, the agreed common requirements have not been complied with for exceptional circumstances, those circumstances and the reasons shall be recorded in writing at the time of the departure from the agreed common requirements and the written record shall be admissible in legal proceedings.

Part IV – Treatment of electronic evidence upon receipt

Article 8 – The requesting party

1. The provisions of this Article apply where the requesting party makes a request for evidence in electronic form to the sending party.

2. When the requesting party makes a request for evidence in electronic form, regardless of the mechanism by which the evidence is requested, the requesting party shall provide a legally binding undertaking in writing to the sending party to include the following:

   (a) An assurance that the data shall be dealt with in accordance with how evidence in legal proceedings is normally dealt in the requesting parties' jurisdiction under the relevant legislation, procedural rules and rules of professional conduct.

   (b) Copies of the data shall only be given to parties authorized to receive the data that are part of the relevant legal proceedings.

   (c) Data provided under the provisions of this Article 8 shall only be used for purposes related to the relevant legal proceedings.

   (d) The sending party may waive the provisions of Article 8(2)(b). The terms of any such waiver shall be decided by the parties in a form and to the extent that they determine.

3. Notwithstanding the provisions contained in Article 8(2) above, all data in electronic form that is provided to the requesting party shall be the subject of all the relevant laws of the requesting party, including, but not limited to, confidentiality, the protection of data and the security of data.

4. The assurances provided by the receiving party under the provisions of Article 8(2) above may be provided in physical or electronic form as is agreed between the parties.

5. The provisions of Article 8(3) shall also apply to any other receiving party authorised to receive the data that are part of the relevant legal proceedings.

Part V – General provisions

Article 9 – Admissibility of electronic evidence from other jurisdictions

1. Where electronic evidence originates in another jurisdiction, its admissibility is not impaired if the electronic evidence is proven in accordance with Article 3 or the authenticity of the evidence is otherwise demonstrated.

2. The provisions of this Article 9 do not modify any domestic rule that applies to evidence in electronic form obtained contrary to relevant human rights legislation or data protection legislation.

Article 10 – Recognition of foreign electronic evidence and signatures

1. In determining whether or not, or to what extent, data in electronic form are legally effective, no regard shall be had to the geographical location where the data were created or used or to the place of business of their creation, provided those data are located in the domestic jurisdiction.

2. Where the electronic record or document is located in a foreign jurisdiction, Article 10(1) above does not apply unless –

   (a) the party who adduces evidence of the contents of an electronic record or document has, not less than 14 days before the day on which the evidence is adduced, served on each other party a copy of the electronic record or document proposed to be tendered, except where exceptional, urgent

and exigent circumstances apply;

(b) the court directs that it is to apply; or

(c) there is an international treaty in effect establishing recognition of electronic records or documents or of electronic signatures located in the foreign jurisdiction.

3. Notwithstanding the provisions of Article 10(2)(a) above, what constitutes exceptional, urgent or exigent circumstances for the purposes of this Article is a matter for the court seized with the matter.

4. Notwithstanding the provisions of Article 10(2) above, an adjudicator may admit data in electronic form that are located in a foreign jurisdiction if domestic law so provides.

Article 11 – Interpretation

1. Where the meaning of a word or phrase in this Convention differs from the meaning of a word or phrase defined in any information technology literature, the adjudicator shall interpret the meaning in accordance with the domestic law on the interpretation of words and phrases.

Article 12 – Entering into force

1. The Convention shall enter into force on the thirtieth day following the date of deposit with the [*name of sponsoring organization*].

2. For each State ratifying or acceding to the Convention after the deposit of the [third] instrument of ratification or accession, the Convention shall enter into force on the thirtieth day after the deposit by such State of its instrument of ratification or accession.

EXPLANATORY NOTES TO THE DRAFT CONVENTION ON ELECTRONIC EVIDENCE

1. The main objective is to pursue a common policy towards electronic evidence, taking into account the differences in the treatment of evidence in individual jurisdictions. This Convention does not seek to harmonize judicial systems. The aim is to encourage judges and lawyers to more fully understand the concept of electronic evidence in the interests of providing for fairness in legal proceedings; to promote adequate procedures in legal proceedings; to implement appropriate legislation where necessary, and to promote international co-operation.

2. Part I Article 1 provides a number of definitions. The aim is to provide definitions that transcend legal cultures. Although the definition of "authentication" does not include reference to relevant international or domestic guidelines and standards, it does not preclude the use of such guidelines and standards in demonstrating authenticity. The definition of "electronic evidence" is taken to be synonymous with the term "digital evidence".

3. Part II considers the status of electronic evidence, covering the admissibility of electronic evidence (Articles 2 and Article 3), authentication (article 4) and best evidence (Article 5).

4. Article 2 aims to provide minimum rules to the admissibility of electronic evidence. The purpose of Article 2(1) is to prevent a party from seeking to exclude evidence in electronic form because it is in electronic form. Article 2(2) does not modify any domestic rule relating to the admissibility of electronic evidence other than in relation to authenticity and best evidence.

5. Article 3, regarding the agreement on admissibility of electronic evidence, is taken and adapted from the *Commonwealth Draft Model Law on Electronic Evidence* and *Electronic Evidence: Model Policy Guidelines & Legislative Texts* (Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean, International Telecommunication Union Telecommunication Development Bureau, Geneva, 2013).

6. The provisions of Article 3(1) aim to permit the parties to a legal proceeding to agree on the authenticity of the evidence. The purpose of Article is to simplify the legal process by reducing the time that might be spent in authenticating documents and records in electronic form that both parties rely on. There is no point in increasing the time (and costs) spent on unnecessary actions.

7. Article 4(1), deals with the process of proving that data in electronic form is what it claims to be. The word authenticity is used, even though this may be considered to be irrelevant and out-of-date. To establish whether a electronic record, document or other thing is proven to be what it claims to be, the tests regarding the integrity, reliability and completeness of the data and therefore trustworthiness is more important. It is for the adjudicator to assess the evidence before them to determine whether the data is what it claims to be. The term "authentic" is used by many jurisdictions in other contexts, such as the provision of an "authentic" record. The word "authentication" remains, but it should not be taken to override the domestic methods of determining whether an electronic record, document or other thing is proven to be what it claims to be – nor does it refer to the "authentic" record.

8. Article 4(2) was initially taken from Stephen Mason,

Electronic Evidence (3rd edn, LexisNexis Butterworths, 2012), 4.21. Both the *Commonwealth Draft Model Law on Electronic Evidence* and *Electronic Evidence: Model Policy Guidelines & Legislative Texts* (Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean, International Telecommunication Union Telecommunication Development Bureau, Geneva, 2013) provide for a presumption (the term "judicial notice" is also used in some jurisdictions – this term has a similar effect to the presumption) that electronic evidence is "reliable" or that a computer system or other similar device was "operating properly". No lawyer or judicial authority has put any evidence forward to establish what "reliability" means in relation to computers and computer like devices, or what "operating properly" means. Because a minority of jurisdictions adopts this presumption in the absence of any evidence that such a presumption is justified, it is considered more appropriate to refrain from including such a presumption in the Draft Convention.

9. The provisions of Article 4(2) operate to require a party to demonstrate whether the data in electronic form it is what it claims to be, and conversely, for the challenging party to cross examine to establish that the data is not an accurate presentation of what it claims to be.

10. Article 5 specifically refers to the common law concept of best evidence. The term "original" has deliberately not been included in this Draft Convention. This is because the word "original" has different meanings for lawyers and notaries, and also in different jurisdictions. The term "original" is not helpful when analysing evidence in electronic form. This is because every item of data in electronic form is a copy. There can be no original.

11. Part III deals with the investigation and examination of electronic evidence in Articles 6 and 7.

12. Article 6 provides for the formal education and training of digital evidence practitioners. People that investigate, seize and analyse evidence in electronic form ought to be educated and trained through a formal process. This is in the interests of justice and fairness between the parties, and because evidence in electronic form is now ubiquitous and an every-day part of legal proceedings.

13. Article 7 provides for the creation of a Forum to develop appropriate guidelines or standards for the process of investigating evidence in electronic form. A number of guidelines exist at present. It is the interests of justice that such guidelines are not only publicly available, but are developed by representatives from internationally respected bodies. By developing a set of internationally recognised guidelines, adjudicators will be better informed when assessing evidence in electronic form. The development of common guidelines or standards will also promote confidence in and acceptance of the quality of evidence especially where obtained in another jurisdiction.

14. Part IV provides for the transmission of data in electronic form between jurisdictions. The terms of Article 8 do not affect the provision of any Mutual Legal Assistance Treaty, bilateral or multilateral instrument, or of any other method of requesting evidence from a foreign jurisdiction. The purpose of this provision is to reassure the sending party that the evidence sent will be dealt with appropriately and in accordance with the norms of the receiving jurisdiction relating to evidence in legal proceedings. Some jurisdictions are wary of sending evidence without suitable provision for the security and the protection of the people mentioned in the data.

15. Part V deals with general provisions. In particular, Article 9 on the admissibility of electronic evidence from other jurisdictions attempts to deal with the difficult question of which set of legal requirements apply to evidence in electronic form – whether it is of the State in which the evidence is geographically located, or the State in which the evidence is to be submitted in a legal proceeding. Article 9(1) seeks to indicate that if the evidence is proven in accordance with the provisions of Article 4, the matter of the geographical location is irrelevant. Alternatively, an adjudicator can admit the evidence as being authentic where the authenticity of the evidence is demonstrated in some other manner that is accepted by the adjudicator.

16. Article 10 provides that evidence in electronic form that ostensibly originates in a foreign jurisdiction can be admitted, notwithstanding that it was not actually located in the domestic jurisdiction. The aim is to enable the admission into a legal proceeding of electronic evidence and electronic signatures that might otherwise not be admitted because of lack of formalities.

17. Although the provisions of Article 11(1) may appear to be open to interpretation, the clause mirrors many such clauses in legislation relating to electronic commerce and communications across the world. Article 11(2) deals with the inevitable disagreement between the meaning of words in a technical sense and a legal sense. When this occurs, it is for the adjudicator to determine the meaning in accordance with the relevant provisions in domestic law on interpretation. There has been no attempt to incorporate technical definitions into the Convention, because doing so might cause greater uncertainty than is intended.

SELECT BIBLIOGRAPHY

A number of documents and studies have been conducted by various agencies in relation to aspects of electronic evidence, some of which have influenced the development of this Draft Convention. They are listed below. Unfortunately, they are limited to the English language. Participants in this exercise were encouraged to add to this list any work undertaken in other jurisdictions and in other languages. The aim was to be inclusive, not exclusive.

For an introduction to the basis upon which this project was formed, see Stephen Mason, "Towards a global law of digital evidence? An exploratory essay" – published in *Revista de Concorrência e Regulação*, Ano VI, number 23-24, julho–dezembro 2015, 239 – 258 and (2015) 103 Amicus Curiae 19-28.

Regional recommendations – European Union

Recommendation No R (81) 20 of the Committee of Ministers to Member States on the harmonisation of laws relating to the requirement of written proof and to the admissibility of reproduction of documents and recordings of computers (Adopted by the Committee of Ministers on 11 December 1981 at the 341st meeting of the Ministers' Deputies).

Recommendation No R (95) 13 of the Committee of Ministers to Member States concerning problems of criminal procedural law connected with information technology (Adopted by the Committee of Ministers on 11 September 1995 at the 543rd meeting of the Ministers' Deputies).

Reports

Bert-Jaap Koops and Morag Goodwin, *Cyberspace, the cloud and cross-border criminal investigation The limits and possibilities of international law*, Commissioned by WODC, Ministry of Security & Justice (Tilburg University, December 2014).

UNODC Comprehensive Study on Cybercrime (United Nations, New York, Draft – February 2013).

Model laws

Electronic Evidence: Model Policy Guidelines & Legislative Texts (Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean, International Telecommunication Development Bureau, Geneva, 2013).

Commonwealth Draft Model Law on Electronic Evidence LLM(02)12.

Projects

European Informatics Data Exchange Framework for Courts and Evidence (CSA (Supporting Action), Call ID FP7, grant agreement number 608185, duration 32 months (March 2014 – October 2016)).

The use of electronic evidence in civil and administrative law proceedings and its effect on the rules of evidence and modes of proof A comparative study and analysis (Stephen Mason, assisted by Uwe Rasmussen)(European Committee on Legal Co-Operation, Strasbourg, 27 July 2016, CDCJ(2015) 14 final).

European Certificate on Cybercrime and Electronic Evidence (ECCE project, Cybex and European Commission, 2007).

The Admissibility of Electronic Evidence in Court (EU AGIS 2005 Programme and Cybex, 2006).

Books

Stephen Mason, ed, *Electronic Evidence* (3rd ed, LexisNexis Butterworths, 2012) [4th edition due in early 2017, and will be a free download in PDF form].

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

George L Paul, *Foundations of Digital Evidence* (American Bar Association, 2008).

Paul R. Rice, *Electronic Evidence – Law and Practice* (2nd ed, American Bar Association, 2009).

Allison Stanfield, *Computer Forensics, Electronic Discovery & Electronic Evidence* (LexisNexis Butterworths, 2009).

LIST OF PARTICPANTS

Carmelo Asaro, retired Italian judge, teaching courses on the degree of Master sulla Sicurezza and Master sul Cyberceime at Departimento di Informatica in the Università degli Studi di Roma "La Sapienza", Rome.

Steven David Brown, Independent law enforcement consultant.

Hein Dries, LLM.

Dr Mark Lomas, Capgemini UK plc.

Dr Steven J Murdoch, Royal Society University Research Fellow in the Information Security Research Group of University College London.

Associate Professor Uldis Ķinis, Rīgas Stradiņa Universitāte.

Tim McCormack.

Angus M Marshall, BSc, CEng, FBCS, CITP, FRSA, Director and Principal Scientist, n-gate Limited; Director, Digital Evidence Virtual Centre of Excellence CIC and Visiting Fellow at the Open University.

Goran Oparnica, Managing Director of INsig2 d o o.

Bertan Özerdağ, Judge of the Kuzey Kıbrıs Türk Cumhuriyeti Yüksek Mahkemesinin (Supreme Court of the Turkish Republic of Northern Cyprus).

Gita Radhakrishna, senior lecturer at the Faculty of Law, Multimedia University, Malaysia.

Dr Giuseppe Vaciago, Partner at R&P Legal and Lecturer at the Faculty of Law, University of Insubria (Como), Italy.

EVENTS

Launch of the Draft Convention on Electronic Evidence, held at DataFocus 2016, Zagreb, Croatia, 5 April 2016.

Workshop on the Draft Convention on Electronic Evidence, held on 20 May 2016 between 14:30 and 17:00 at the Institute of Advanced Legal Studies, 17 Russell Square, London WC1B 5DR. Attendees: Michael Asher, Barrister; Werner R Kranenburg, Attorney and Counselor-at-Law, Krenenburg; Dr Alan McKenna, Associate Lecturer, Law School, University of Kent; Naraindra Maharaj, Datatec Financial Services Limited;Nikolaos Trigkas, LLB, MBA, PhD in Law candidate (University of Aberdeen); Katrine Broch Petersen; Dr Michael Reynolds, Solicitor and Arbitrator; Dr Judith Townend, Director, Information Law and Policy Centre, Institute of Advanced Legal Studies, London; Richard Trevorah, tScheme Limited.

ACKNOWLEDGEMENTS

A brief introduction to the development of this Convention can be read here: Stephen Mason, "A proposed Convention on Electronic Evidence", *Pandora's Box*, 2016, 153 – 155 (http://www.jatl.org/pandoras-box/). I was invited by the L'Accademia di Diritto Europeo – Academy of European Law – Europäische Rechtsakademie – l'Académie de droit europée to speak at an event entitled "Relying on Electronic Evidence in Criminal Cases" (event number 315DT21) held in Bucharest on 12 and 13 November 2015 at the Institutului National al Magistraturii. One of the attendees asked a question that is often asked at similar events: "Why was there no Convention on Electronic Evidence?" My usual response was that no organisation wanted to spend the time developing one, but on this occasion, I decided at this event to write one myself, and announced that this is what I was going to do.

Part of the content of this Draft Convention on Electronic Evidence was taken from the *Commonwealth Draft Model Law on Electronic Evidence and the Commonwealth Draft Model Law on Electronic Evidence and Electronic Evidence: Model Policy Guidelines & Legislative Texts* (Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean, International Telecommunication Union Telecommunication Development Bureau, Geneva, 2013). These valuable sources are explicitly recognised, as is their copyright. I wrote the remainder of the first version of the text.

I am not technically competent, so I was very fortunate that Hein was able and willing to host the web site using the domain name I registered for the purposes of the development of the Convention (conventiononelectronicevidence.org).

My first thanks go to Hein for taking on this arduous task while continuing to work his way around Europe fulfilling various contracts, and also commenting on the content of the Convention.

I also thank the Institute of Advanced Legal Studies for hosting the workshop held in London. It was a useful event.

A final word of thanks to everyone that took the time to read the various iterations of the Convention and offer comments. As can be imagined, lawyers and technicians tend to use language in different ways, and the discussions partly reflect this. I have approached the task of redrafting text by taking into account these differences, and adjusting words where they can be adjusted to the benefit of the project without loosing meaning.

Some suggestions have been made that do not appear in this draft Convention. Their failure to appear is not because they were irrelevant. In drafting a Convention, it is important to ensure that the text can be generally agreed. This means excluding controversial provisions that are not universally shared.

Stephen Mason, 2016

Stephen Mason

Barrister; Associate Research Fellow, IALS