ARTICLE:

Problems on the admissibility of electronic evidence in the Chinese context

By **Bo Liu**

Some Chinese scholars and practitioners propose that original physical items should be the subject of one of the exclusionary standards. Starting from this premise, this article analyses the pitfalls caused by the preference for original evidence, and the reasons for the rigorous standard of admissibility for electronic evidence in Chinese judicial practice. This includes a misunderstanding of the theory of admissibility for electronic evidence, indicating a misunderstanding between admissibility and probative value. This view is influenced by the criminal evidentiary standard, neglecting the important function of authentication, and the lack of knowledge of electronic evidence. That it is easy to alter or tamper with electronic evidence goes to the weight rather than the admissibility of the evidence. Electronic evidence can be authenticated by other circumstance evidence,[1] rather than preventing suspicious evidence from being admitted into legal proceedings.

The digital world has become a main source of evidence, and the admissibility and the weight of electronic evidence has become an unavoidable issue for lawyers and judges.[2] However, because electronic evidence is not a physical object, but only exists as digital data stored on tangible carriers, there is an argument in China over which kind of electronic evidence is reliable and authentic.

On 12 October 2014, law school of Peking University and Shandong Criminal Bar Union jointly proposed exclusion rules for criminal cases, in which they tried to guarantee the authenticity of electronic evidence by providing for the original physical items storing the data, together with a written statement concerning the evidence. The *Illegal Evidence Exclusion Guide of Criminal Cases for Defense Lawyer (tentative)* was published, in which article 11 proposed that audio-video evidence and electronic evidence should be excluded under the following circumstances:

> (1) where there is no explanation about its collection process, and where it is collected through illegal methods;
>
> (2) where it is presented without the original physical items;
>
> (3) where it is collected or duplicated by a single investigator, which is not sufficient to guarantee the integrity of the evidence;
>
> (4) where there is no written statement about its collection, image process, and the location of its original physical items, or the written statement is not signed properly.

However, although important, the original physical item of storage is not the only determining element for the authenticity of electronic evidence. Such a proposal reflects a misunderstanding towards the conception of 'original' in terms of electronic evidence, and without a clear definition of what the original is, valuable electronic evidence would be excluded inevitably. But this is not the only problem concerning the admissibility of electronic evidence. The Interpretation of the Supreme People's Court on the Application of the Civil Procedure Law of the People's Republic of China, issued on 30 January 2015, emphasized, in article 116 that:

> 'electronic data is the information in the form of email, electronic data interexchange, online chat records, blogs, short message, electronic signature, domain name etc, and the information stored on electronic mediums.'

Chinese laws have admitted that electronic data was a form of legitimate evidence previously.[3] The

[1] For which see Stephen Mason, ed, *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012) chapter 4.

[2] This is illustrated by the editorials over the years in the Digital Evidence and Electronic Signature Law Review. In particular, see Denise H. Wong, 'Educating for the future: teaching evidence in the technological age', 10 *Digital Evidence and Electronic Signature Law Review* (2013) 16 – 24 and Deveral Capps, 'Fitting a quart into a pint pot: the legal curriculum and meeting the requirements of practice', 10 *Digital Evidence and Electronic Signature Law Review* (2013) 23 – 28.

[3] In 2010, Provisions of the Supreme People's Court, the Supreme People's Procuratorate, the Ministry of Public Security, the Ministry of State Security and the Ministry of Justice on Several Issues Concerning the Examination and Judgment of Evidence in Handling Death Penalty Cases clarified that e-mail, electronic data interexchange, online chat records, blogs, short message were electronic evidence, which is the first time that electronic evidence was mentioned clearly in Chinese statutes. Then the newest procedure laws, including the Criminal Procedure Law (2013), the Civil Procedure Law (2013) and the Administrative Procedure Law

reiteration of the conception of electronic evidence indicated that the courts were reluctant to rely on electronic evidence to make the decision.[4] The aim of this paper is to discuss the main problems relating to the admissibility of electronic evidence in China and analyse the probable causes.

Admissibility influenced by the preference for originals

To secure the authenticity and credibility of evidence, an exhibit should be original. For example, article 70 of the existing Civil Procedure Law (2013) provides that any documentary or material evidence shall be submitted in its original form, and article 22 of Some Provisions of the Supreme People's Court on Evidence in Civil Procedures (2001) require that computer data, a voice record or video should be collected with their original carriers. Some regulations also stipulate the weight of electronic evidence, such as article 64 of the Supreme People's Court Regulations on Several Issues concerning Evidence in Administrative Procedures (2002), which provide that electronic data interchange, e-mail or other data object fixed or displayed on tangible items would have the same value as the originals have when their production and authenticity can be affirmed by the opposing party, or verified by other effective means, such as by a notary. Article 5 of the Provisions on Evidentiary Issues in all kinds of Cases, issued by the Higher People's Court of Beijing (2001) had similar stipulations. One researcher has said that the authenticity of electronic evidence was bound up with its primitiveness, and the concept of original played an important role in deciding the authenticity, so authenticity should not be isolated from the concept of 'originals',[5] these laws reflect the same consideration. So much emphasis is put on original items by legislators and practitioners that it is not hard to conclude that it is the preference for originals that resulted in the idea of adopting original physical items as the admissibility standard.

The significance of producing the original copy of electronic evidence lies in the metadata or a data fingerprint, which can be very useful and important for the authentication of electronic evidence. In August 1998, the Scientific Working Group on Digital Evidence[6] defined original digital evidence as physical items and the data objects associated with such items at the time of acquisition or seizure.[7] By this definition, we can tell that the range of electronic evidence is not limited to those with original physical items but includes all digital data in whatever form. This is not difficult, because although electronic evidence is always associated with physical items, the storage medium may be difficult to identify or present at trial. For instance, e-mails, web-based instant chat records, web pages, cloud stored information etc, the 'original' can only be their digital content at the time of collection, which may occur in different formats without altering the original information. This means it is not possible to say which one is the 'original' or how many 'originals' exist. Therefore, the physical item of storage is just a part of the 'original' of electronic evidence, and the traditional standard for original and their copies do not apply in the digital world. Mason explained this in a haiku, which was published in his text *International Electronic Evidence* (haiku cited with permission of the author):[8]

Original

Rain droplets land, merge,

divide on petals of the

Somei Yoshino.

Mason later explained the meaning of this haiku in an essay.[9]

Due to the preference for original documents and the complexity of identifying the original, some people would rather choose a simple way to decide the

(2015) all admit the legal status of electronic evidence, by adding 'electronic data' in the definition of 'evidence'.

[4] Although see *Yang Chunning v Han Ying*, (2005) hai min chu zi NO.4670, Beijing Hai Dian District People's Court, where text messages proved a loan, and the typed name at the end of the messages were an electronic signature, translated into English and published in the *Digital Evidence and Electronic Signature Law Review*, 5 (2008), 103-105.

5 Wenyan He, Qinglin Zhang, 'Research of the Classification and Authenticity Judgement of Electronic Data', *Journal of Xiangtan University (Philosophy and Social Sciences)*, 2013(2), 31-37.

[6] In this definition, 'digital evidence' is used in original text in this paper. While the term 'electronic evidence' is commonly used to denote digital evidence, it is a generative term, rather than a specific term, in that it encompasses all forms of data, whether produced by an analogue device, or in digital form. See Stephen Mason, 'Digital Evidence in Five Nations' (appendix D) in George L. Paul, *Foundation of digital evidence* (ABA Publishing, 2008), at 258 and Burkhard Schaffer and Stephen Mason in Stephen Mason, ed, *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012), 2.01 – 2.03.

[7] Carrie Morgan Whitcomb, 'An Historical Perspective of Digital Evidence: a forensic scientist's view', *International Journal of Digital Evidence*, Spring 2002 Volume 1, Issue 1.

[8] (British Institute of International and Comparative Law, 2008).

[9] '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 at http://sas-space.sas.ac.uk/2565/ .

authenticity and admissibility of electronic evidence, equalling the concept of 'original physical items' to the concept of 'originals', but they neglected the difference between them, and the special characters of electronic evidence. Electronic evidence is different from video or audio evidence in analogue format, which is in the form of physical evidence, and can be relatively easy to identify.[10] The adoption of the concept of an original physical item as the basis of the exclusionary criteria for electronic evidence diminishes the concept of electronic evidence, and eliminates the possibility of producing or admitting electronic evidence with probative value.

Reasons for the rigorous admissibility standard

That the original physical items acts as the crux for the inclusion or exclusion of electronic evidence reflects the cautious attitude towards electronic evidence of Chinese scholars and practitioners. Also, in practice, whenever there is an objection from the opposing party or there is any uncertainty about the origination or authenticity of electronic evidence, the electronic evidence is likely to be excluded by procurators or judges. To better understand the application of electronic evidence in China, 50 civil cases that included different sources of electronic evidence separately, including blogs, chat records, web pages and e-mail, were picked randomly from a case database[11] and analysed. It was found that electronic evidence was only admitted in about 60 per cent of the cases.[12] The common reasons for judges to exclude electronic evidence are that the evidence is a copy or a print of a copy, so its authenticity cannot be verified, and the evidence may be generated by others.[13] From this point, we can see that the admissibility of electronic evidence is much more rigorous in Chinese judicial practice than in other legal systems.

For instance, in the United States of America, the prerequisite of authentication only needs a prima facie showing of reliability, which is not difficult to satisfy.[14] In what can be called the continental law system, the admissibility for electronic evidence differs between jurisdictions.[15]

The possible causes in China are discussed below.

Misunderstanding the difference between admissibility and weight

The more relevant information collected, the more precisely the facts can be ascertained, so some information should not be excluded recklessly due to its uncertainty. Physical evidence or paper documents can be forged, and the witnesses' competency can be questioned due to their youth or perceptive defects,[16] but all these elements would affect only the weight of the evidence, not the capability of giving evidence. Similarly, electronic evidence should not be excluded simply because of its vulnerability to being tampered or altered. Many courts in the United State of America have held that the mere possibility of alteration is not sufficient to exclude electronic evidence, in the absence of specific evidence of alteration. Such possibilities goes only to weight, not admissibility.[17] In Germany, electronic evidence is usually regarded as preliminary evidence, and the admissibility and

[10] Video and audio evidence is one of the eight kinds of legal evidence. Long before admitted as legal evidence by law, digital data was usually treated in the same way as video and audio evidence by Chinese legislators.
[11] http://www.pkulaw.cn/Case/ .
[12] In this statistics, the ratio of the admitted blogs, online chat records, QQ chat records, WeChat records, web pages and e-mail is 60 per cent, 40 per cent, 58 per cent, 68 per cent, 60 per cent and 62 per cent separately. And one of the main reasons for admitting the evidence is the absence of objections from opposing parties.
[13] For example, in a trademark infringement case ((2015)甬仑知初字第6号), the defendant denied the authenticity of the photograph of the brake pad because it was a printout, so the court excluded it during its decision making; in a contract dispute case ((2012)甬余泗商初字第529号), the defendant company presented a printout of chat records between its own salesperson with another salesperson from the plaintiff's company, the plaintiff argued that the defendant could not prove that the records were produced by the persons that purported to be, the courts accepted the objection and excluded the evidence.
[14] Jonathan L. Moore, 'Time for an Upgrade: Amending the Federal Rules of Evidence to Address the Challenges of Electronically Stored Information in Civil Litigation', 50 *Jurimetrics* 147 (2010).
[15] For which see Stephen Mason, gen ed, *International Electronic Evidence* (British Institute of International and Comparative Law, 2008), and Stephen Mason, 'Digital Evidence in Five Nations' (appendix D) in George L. Paul, *Foundation of digital evidence* (ABA Publishing, 2008), at 236.
[16] Article 60 of the Chinese Criminal Procedure Law (2013) stipulates that physically or mentally handicapped persons or minors who cannot distinguish right from wrong or cannot properly express themselves shall not be qualified as witnesses.
[17] For example, some defendants have argued that e-mails and on-line chat records should not be admitted because they were incomplete, easily altered, or possibly from an unidentified third party, but the court has usually held that such issues touched upon concerns regarding the weight of given evidence and not its authenticity, for which see Scott R. Grubman and Robert H. Snyder, 'Web 2.0 Crashes Through the Courthouse Door: Legal and Ethical Issues Related to the Discoverability and Admissibility of Social Networking Evidence,' *Rutgers Computer & Technology Law Journal,* 2011 Spring-Summer; 37(1-2); Computer Crime and Intellectual Property Section, 'Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations', published by the Office of Legal Education Executive Office for United States Attorneys, 2009, at 202.

probative value is decided by judges' discretion. Authenticity and integrity are two main factors in evaluating its probative value.[18] In brief, both in America and Germany, the uncertainty of electronic evidence affects the weight and not the admissibility.

It is suggested that to adopt high admissibility criteria for electronic evidence and to exclude such evidence due to the insufficiency of authenticity misses the difference between the admissibility and the weight of electronic evidence. This seems to be the case in China. A survey of 69 criminal judges (including assistant judges) from a northern city in China showed that in criminal cases, when evaluating electronic evidence, quite a portion of judges do not distinguish between admissibility and weight because of lack of awareness, or for avoiding unnecessary troubles. They determine the admissibility and the weight at the same time. In addition, many judges did not know how to evaluate admissibility and weight.[19]

Under the influence of evidentiary standards of prosecution

According to the provisions of article 172 of the newest amendment of the Criminal Procedure Law of the People's Republic of China (2013), when the people's procurator considers that the facts of a crime have been ascertained; that the evidence is reliable and sufficient, and that criminal responsibility should be charged according to the law, it is required to make a decision to initiate a prosecution. According to this article, the evidentiary criteria for a criminal indictment is that the evidence is reliable and sufficient, which is a relatively high bar, and almost equal to the proof standard of achieving a conviction. The position is made more complex, because in practice, the rate of indictment and guilty verdicts were adopted as the main assessment index for promotion.[20] This meant that electronic evidence was more difficult to adduce in criminal proceedings because authenticity tends to be questioned in multiple ways. Affected by this judicial environment, other legal personnel, such as lawyers and judges, are likely to treat electronic evidence with a more cautious view, which means they prefer that its authenticity can be testified clearly. The main issue in any contention over truth is not the concept of admissibility, but the weight of their evidence.[21] The indicting criteria for criminal cases is the unilateral demand of evidence by the procuratorate, and the exclusion of some electronic evidence is based on the comprehensive evaluation of the whole case materials. So it is argued that the evidentiary criteria to draw up an indictment should not be adopted as the same criteria for the court to admit or exclude evidence.

The absence of authentication procedure for electronic evidence

Lawyers and prosecutors have a duty to collect and preserve evidence and defend its admissibility. The authentication procedure, which is designed to indicate the credibility of evidence, has vital significance in deciding the admissibility and the weight of the evidence, because only evidence with seemingly credibility can be admitted and the possibility of credibility in turn decides the weight. Taking the particular features of electronic evidence into account, authentication is of more importance. In some American courts, judges have excluded electronic evidence for lack of foundation, but it is important to note that the judicial approaches vary.[22] In Chinese judicial practice, electronic evidence should be submitted with other relevant evidence that can explain the generation of the electronic evidence, or corroborate and support the electronic evidence in a way that it forms a complete chain of evidence.[23] The Chinese judicial system has not adopted authentication as a mandatory procedure for admissibility. In addition, at present, there is no legislated authentication procedure for evidence, especially for electronic evidence in the Chinese trial process. Objectivity has long been hailed as one of the three basic requirements[24] for admitting evidence in the Chinese judicial system. This means that because objectivity and authenticity were so close, authenticity is given the superficial appearance of objectivity. It is suggested that a procedure for authentication should exist in the Chinese trial system

[18] Alexander Duisberg and Henriette Picot, 'Germany', in Stephen Mason, ed, *International Electronic Evidence* (British Institute of International and Comparative Law, 2008) at 337.
[19] See Zhufeng Li, 'From legislation to judicature: electronic evidence evaluation in criminal procedure', *Academic Exchange* (2013) (7), 35-37.
[20] The Central Political and Legal Affairs Commission of the Communist Party of China demanded all kinds of legal organs to revoke such criteria in January 2015.
[21] George L. Paul, *Foundation of digital evidence* (ABA Publishing, 2008) at 49.
[22] Sheldon M. Finkelstein and Evelyn R. Storch, 'Admissibility of Electronically Stored Information: It's Still the Same Old Story', 23 J. Am. Acad. Matrimonial Law 45, 2010.
[23] Prosecutor Speaks on Qin Huohuo Case: Electronic Evidence is a Double-edged Sword, http://news.jcrb.com/jxsw/201404/t20140417_1375000.html.
[24] The other two requirements are relevance and legality.

as a method to secure and approach the objectivity standard.

In addition to introducing electronic evidence itself, an authentication procedure requires the proponent to present other collateral evidence to support the authenticity of electronic evidence.[25] Without an appropriate authentication process, and the tendency of the opposing party to object to electronic evidence without grounds, the judges, who lack knowledge and expertise with electronic evidence, can easily be confused when evaluating the credibility and the weight of electronic evidence. The reasons behind the absence of an authentication procedure range from the judicial tradition in which witnesses are unwilling to testify in court, to the vagueness in legal consequence for false testimony, perjury, and the destruction of evidence, and the vagueness about the roles and legal responsibilities of internet service providers in reserving and producing electronic evidence for judicial activities. All of these factors should be considered seriously because electronic data is usually stored or traced via a third party and is vulnerable to being altered or deleted.

Witnesses not testifying in court

The advantages of in-court testimony are that the judge can examine the sincerity of the witnesses by observing them face to face and make inquiries concerning any confusion or ambiguity in the narrative of evidence. The most frequent ways to authenticate electronic evidence are witness with personal knowledge, distinctive characteristics,[26] expert testimony, comparison with an authenticated exemplar, system or process capable of producing a reliable result, and self-authentication.[27] The content of such testimony is mostly out of the judges' field of knowledge. This means it is not practical for judges to decide on the reliability and the weight of electronic evidence based on a complicated written statement. It is therefore of great importance that the opposing party can cross-examine the witness, or the judge can inquire the witnesses at trial. Besides lay witnesses, expert witnesses are more necessary in order to make the judges understand electronic evidence. The testimony of a qualified digital evidence specialist helps to educate the judges. However, the ratio of witness testifying in court in criminal cases in China was less than 1 per cent before 2013, while the newest revised Criminal Procedure Law has not made the ratio a significant improvement, although it establishes the compulsory attendance of the witness.[28] Such a low ratio of testifying witnesses in court in China directly affects the authentication procedure of electronic evidence.

Penalty for false testimony and destruction of evidence

Compared with paper documents or other physical evidence that possess a tangible appearance, the authentication of electronic evidence in China is dependent on the assessment of the sincerity of the witness. This is because the content of electronic evidence is purely digital data of which such issues as the origination, the time of creation, name of creator are difficult to determine. Also, it is not always easy to discover whether or not electronic evidence has been deliberately altered, or tampered with by the witness, parties or other third parties. Sincerity is related to the witnesses' personal quality, and can be the result of deterrence by law, and deterrence is especially important in China where the sincerity of the general public is relatively low. But in China, the penalty for false testimony mostly focuses on criminal charges rather than civil action, and among the criminal charges, only those causing severe results are punished. Such laws are deficient, and have lead to the fact that very few witnesses who give false testimony are given criminal sanctions in practice. Under such circumstances, false statements may exist abundantly in the collateral evidence used to support the reliability of electronic evidence, and thus makes judges reluctant to adopt such a procedure, which leads to a preference for other authenticating methods, such as reports from forensic experts or notaries.

[25] The origination, generation process, creator and producing time, and the fact of being unaltered after collection and the proof of integration of electronic evidence are all important elements supporting the authenticity. Each of these elements can be supported by circumstantial evidence. Even if the admissibility of electronic evidence is not a problem, they are still vital to judge the weight of the evidence. This is covered extensively in Stephen Mason, ed, *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012) chapter 4.

[26] Such as user name, e-mail address, identity, nickname, specific content mentioned in communication, Hash value, marks, and metadata etc.

[27] Michael D. Gifford, 'Admitting Electronic Evidence in Federal Court: I've Got All This Electronic Data, Now What Do I Do With It?' *AM. B. ASS'N* 2 (2008), http://www.americanbar.org/content/dam/aba/events/labor_law/basics_papers/elst/lied.authcheckdam.pdf .

[28] Zhiwei Lan, Jingping Yu, 'On the New Criminal Procedure Law of Witness System in the Attorney Practice', *Hebei Law Science*, 2013 Sep; 31(9).

The role and legal responsibilities of internet service providers

It is suggested that to preserve and provide digital information should be a legal obligation for internet service providers. According to the Regulation on Internet Information Service of the People's Republic of China (2000), Internet Content Providers (ICP) should provide the content information as well as its publishing time, IP address, domain name and switching information; and Internet Service Providers (ISP) should record and preserve the user's information including the on-line time, account number, IP address or domain name, dialling number. All these providers should keep the data for at least 60 days, and make such information available at the government's request. Based on the interpretation of these regulations, the legal duty of these providers to provide information for government investigation or judicial procedure seems to be too narrow. For example, questions such as whether a public e-mail service provider should disclose the content of e-mails of its users and under what circumstance they should disclose were not mentioned in the regulation, and the expression that internet service providers 'should record and preserve information' implies that it is not a mandatory responsibility for them to provide the digital information, nor to provide testimony to support its reliability. In contrast, in America, internet service providers are required to provide information to law enforcement agencies. Their employees provide affidavits or testimony about the collection or production process of the information when necessary, and this scenario is so common that major internet service providers have a special department to handle these requests.[29] Because internet service providers act as neutral third parties, digital information provided by them is more credible and requires relatively simpler authentication procedures, so the role of internet service providers as electronic evidence providers should, it is suggested, be developed in Chinese judicial practice.

Absence of necessary knowledge

Digital data is pure data, and it can be difficult to determine its origin, creator and modification after its formation and to identify its authenticity and integrity. Hence it is of no surprise and a natural reaction is for people to treat electronic evidence with tremendous caution. When a lawyer wishes to establish facts that original evidence can prove, the lawyer should not rely on irrelevant evidence to prove such facts. For instance, in the case of *Perforaciones Maritimas Mexicanas S.A. de C.V. v. Seacor Holdings, Inc*[30] before Kent J in the United States District Court, S.D. Texas, Galveston Division, the plaintiffs sought to prove there was in existence a joint venture. They did not produce the relevant documents as proof, but referred the court to publications from the internet. This was not accepted by the judge, partly because the contract was not provided to the court, and it was not appropriate to use information from the internet as proof.

But an interesting survey found that less technically aware judges were more wary of electronic evidence than their more technically knowledgeable peers,[31] which shows that the attitude of judges towards electronic evidence is closely related with their understanding or comprehension of modern computer technology. Thus, whether or not electronic evidence can be applied appropriately is decided by not only its characters, but also the attitude and knowledge of people towards it. As far as the situation in China is concerned, the application of electronic evidence has only recently obtained the necessary attention, and the basic electronic evidence training programs at a national level for forensic technicians of police and procuratorate's investigation departments only began in 2014, while lawyers and judges are still not trained. But because of the absence of the necessary knowledge about electronic evidence, lawyers do not know how to present electronic evidence properly, or how to support its authenticity and credibility with other circumstance evidence, while the easiest way for judges is to exclude the evidence whenever opposing parties question it, even when the objection might be unreasonable.[32] So training for judges is necessary because they need basic necessary knowledge to eliminate the mystery of electronic evidence when dealing with such

[29] Michael J. Hannon. *Digital Evidence-computer forensics and legal issues arising from computer investigations* (William S. Hein & Co., Inc., 2012), at 331.

[30] 443 F. Supp. 2d 825, 832 (S.D. Tex. 2006).

[31] Gary C. Kessler, 'Judges' awareness understanding and application of digital evidence', *Journal of Digital Forensics, Security and Law,* 2011; 6(1), 55.

[32] In China, such kind of objections on electronic evidence are common, including: (1) general objection to the relevance, authenticity and legality of the electronic evidence, (2) objection to the form of the printout because it has not been notarized, (3) denying the authenticity due to the evidence is a printout, not the original, etc.

evidence. Training for lawyers is urgent because they should be competent in dealing with technical evidence and educate judges with relevant knowledge during the trial.[33]

Conclusion

Notwithstanding the requirement regarding the need for an 'original' in physical items imposes strict restrictions on the admissibility rules of electronic evidence which can subsequently lead to substantial injustice, especially in internet fraud cases. Although the rules of evidence do not come into play until after the evidence is introduced into court, the rule of exclusion can, and should, influence the entire collection and discovery process of evidence. It is suggested that the draft of the exclusionary rules should be considered with great caution, and the scope of admissible evidence should not be reduced, or the process of proof be simplified due to the absence of knowledge regarding electronic evidence. Secondly, the authentication procedure should be put into force, and best practice guides should be available for lawyers and parties to legal proceedings. The aim should be to fulfil the authentication procedure properly. Finally, the practitioners' sense of mystery towards electronic evidence should be changed through appropriate self-study or training; judges should be authorized to adopt any forms of electronic evidence and allowed to invite suitably qualified digital evidence specialists to help them to evaluate the weight of the electronic evidence when necessary.

Bo Liu, is a Ph.D. Candidate of the Institute of Evidence Law and Forensic Science at the China University of Political Science and Law.

boluomail@163.com

[33] See the editorials: Editorial, 7 *Digital Evidence and Electronic Signature Law Review*, (2010), 5-6, available at http://journals.sas.ac.uk/deeslr/article/view/1917/1854; Editorial, 9 *Digital Evidence and Electronic Signature Law Review*, (2012), 5-6, available at http://journals.sas.ac.uk/deeslr/article/view/1984/1921; Editorial, 9 *Digital Evidence and Electronic Signature Law Review*, (2013), 6, available at http://journals.sas.ac.uk/deeslr/article/view/2012/1949 .