ARCHIVES AND MANUSCRIPTS
2020, VOL. 48, NO. 3, 300–327
https://doi.org/10.1080/01576895.2020.1822892

Routledge
Taylor & Francis Group

ARTICLE

Sitting in limbo or being the flaming Phoenix: the relevance of the archival discipline to the admissibility of digital evidence in China

Weimei Pan[a] and Luciana Duranti[b]

[a]School of Management, Tianjin Normal University, Tianjin, China; [b]School of Information, University of British Columbia, Vancouver, British Columbia, Canada

ABSTRACT
This article presents a review of the progress made in the digital transition in China, especially in light of the fact that admissibility of digital records in legal proceedings is a critical factor in such transition. It discusses the Chinese legal system and the rules governing the admissibility of both paper and digital records as well as the reasons why evidence collection and preservation by a third party has become a popular approach to guarantee the integrity of the records and improve their chances of admissibility in a court of law. In this context, this article then discusses how the InterPARES Trust PaaST model can help address some of the issues, thus, demonstrating the relevance of archival knowledge to the digital transition.

KEYWORDS
PaaST; digital transition; digital records; evidence; China

Background

Electronic records management in China has undergone more than two decades of development since the establishment of the Leading Group on Research on Digital Records Archiving and Transfer[1] and Digital Archives Management by the National Archives Administration of China (NAAC) in 1996.[2] Numerous research projects have been conducted to explore the full life-cycle management of digital records[3] from creation to long-term preservation. Yet, in practice, it appears that only few institutions and programs have completely replaced paper records with digital records with the majority adopting a wait-and-see attitude.[4] A recent survey conducted by one of the authors of this paper shows that, over the past five to 10 years, 66% of the records managers and archivists who answered the questionnaire indicate that the majority of records in their organisations is archived in paper form while only a small portion is archived in digital form, and merely 6% indicate that the majority of records is archived in digital form and a small portion is archived in paper form.[5] The transition from paper to digital records management has been considerably slow in China.

One of the cited reasons for the prolonged transition is the existence of a dual-track and dual-copy system,[6] which is a transitional strategy adopted at the end of last century to temporarily address the issues presented by a widespread use of information technology in the conduct of business and legislations, management principles, and methods

CONTACT Weimei Pan weimeipan3@gmail.com

that lag behind the advancement of information technology and need to be updated for the recognition, assessment, maintenance, and long-term preservation of the trustworthiness of digital records.[7] This strategy is needed to ensure that the evidentiary capacity of records can be protected and demonstrated so that they can be used to show an organisation's regulatory and legal compliance and protect its interests in legal litigations,[8] while the state, lawyers, archivists, and records managers strive to close the legislative, regulatory, and methodological gap.

The dual-track system involves using both the paper and digital version of each record in the conduct of business activities.[9] The degree to which the paper and digital versions participate in the handling of the business matter may vary from case to case. This means that, the two versions may be used simultaneously and independently, or alternatively and exclusively, and this may affect the completeness of documentation as well as the reliability of each record in terms of truly reflecting the business activity producing it.[10]

While the dual-track system concerns the use of information technology in carrying out business, the dual-copy system concerns the management of digital records when the business activities in which they participate are completed. More specifically, it refers to the generation of a paper or microfilm copy of the digital record and the maintenance of both versions when the digital record is transferred into the internal Archival Units for recordkeeping.[11] It is a passive strategy for the management of the large volume of digital records created when there is a lack of mature principles and methods for their reliable and authentic capture, maintenance, transfer, and long-term preservation, and when their admission in court as evidence and their probative force in fact-finding cannot be fully guaranteed.

The kinds of digital records that have to be maintained in dual copies vary according to different regulations; in general, the system is used for digital records with permanent or long-term preservation value, as it was designed to ensure the authentic preservation of digital records.[12] A critical issue with the dual-copy system is that the reliability and authenticity of the paper copy generated cannot be guaranteed, considering that the paper version either does not participate in the business activity and is only, at best, an authentic copy of the original digital record, or only partially participates in the business activity and therefore documents only part of it.[13] Other drawbacks include a waste of resources, difficulties in generating the paper or microfilm copy of some digital records, loss of digital records, the co-existence of a paper records management system and an electronic records management system, and the danger of losing the evidentiary capacity of digital records.[14]

As transitional strategies, the dual-track system and the dual-copy system were enthusiastically embraced by scholars and practitioners in the Chinese records and archives management field in the early 2000s.[15] However, recently, more and more scholars and practitioners are emphasising the limitations and drawbacks of these two systems and announcing that it is time that the dual-track system and dual-copy system be reformed to reflect the developments of the past decade in the management and long-term preservation of digital records and to promote China's digital transition.[16] The changing attitude towards the dual-copy system, in particular, is also reflected in the recent update to state regulations and policies, which either removed the requirement for use of dual-copy system or require the exploration of one-track and one-copy system.[17] Additionally, other contextual factors pushing for the elimination of paper records

include, for instance, the implementation of the 'Digital China' initiative and advancements made in the legal and judicial field.

Due to this circumstance, in the Chinese records management and archival field, digital transition is somewhat equivalent to the abandon of the dual-track and dual-copy system, and the implementation of the one-track or one-copy system, depending on different interpretations of the substance and the scope of these two concepts. And it is not entirely incorrect to say that the actual transition from paper to electronic records management only started recently.

In light of this tendency to replace the dual-track and dual-copy system with a one-track or one-copy system, Chinese scholars and practitioners are researching and writing on the conceptual foundation and the implications of the adoption of a one-track or one-copy system, and on the factors influencing the shift from the dual-copy system to the one-copy system.[18] A frequently cited factor influencing the transition to electronic records management is the admissibility of digital records in legal proceedings.[19] Many legislations and regulations have acknowledged the effectiveness of digital records in the conduct of business activity and affirmed that digital archives that meet archives management requirements should have the same legal force as paper ones.[20]

Yet, it is one thing for the law to acknowledge the effectiveness of use of digital records, and another to expressly admit them as evidence in legal proceedings.[21] While Chinese academics are concerned about the former, it is the latter that they should focus on, so that digital records can be managed accordingly to improve their admissibility in a court of law and eventually promote digital transition. Further, current developments of the discussion over the admissibility of digital records in civil proceedings in the Chinese law and judicial field appear to further complicate the issue and can have an adverse effect on the records management and archival field.

This article presents research conducted to answer the following questions:

(1) What is the judicial landscape for the admission of digital records as evidence in civil cases in China?
(2) Can the identified issues be addressed using archival knowledge?

The sources of data for this article include legal and archival literature, legal statutes, and legal rulings. The article also discusses how the Chinese records and archival field can demonstrate its expertise in protecting and demonstrating the integrity of electronic data by illustrating how archival knowledge – in particular, the ITrust PaaST model – can be used to enhance the rigour of a popular method used for evidence collection and preservation, i.e., the collection and preservation of records by a third party.

Literature review

The evidentiary capacity of records, which supports the continuity of society and guarantees people's entitlement to properties, rights, and privileges, has been at the core of records management since ancient times.[22] Ensuring the reliability and authenticity of digital records is a challenge that has spawned a large body of research. To effectively address it, the records and archives management field has collaborated with the legal and law enforcement field to become cognisant of the application of the law of

evidence and to design policies, procedures, and methods for the lifecycle management of records capable of satisfying the legal requirements for evidence. In the process, legal professionals and scholars are acquiring a grasp of the ways in which information technology can be in compliance with the existing law of evidence and the law of evidence can be amended to maintain its relevancy and adequacy.[23]

In her doctoral dissertation, Heather MacNeil examined and compared the methods for assessing the trustworthiness of records in the fields of law, history, and archival diplomatics,[24] thus, laying the conceptual foundation for collaboration between the law and archival fields. The Law of Evidence in the Digital Environment (LEDE): Finding Solutions to Present and Future Challenges project (2012–2015),[25] a collaboration between the Faculty of Law and the School of Library, Archival and Information Studies (SLAIS) at the University of British Columbia, explored the problem of 'how the law of evidence can address the widening gap between advances in digital record-keeping and the traditional rules of evidence'.[26] Duranti and her colleagues examined the adequacy of the *Uniform Electronic Evidence Act* in Canada in dealing with the complexity of the records created, used, or stored in the digital environment, arguing that the nature and characteristics of electronic records require collaboration among records professions, legal and law enforcement professions, and the information technology profession. Additionally, in his doctoral dissertation, Donald Force explored whether the adoption by an organisation of a recordkeeping standard could be one of the grounds for admission of electronic records as evidence.[27]

In the Chinese records and archives management field, literature on the evidentiary capacity of electronic records began to emerge in the late 1990s, and its volume increased in recent years with the amendment to the criminal, civil and administrative procedural laws[28] and the enactment of juridical interpretations of the admission of electronic data as evidence. While most of these writings aim to facilitate the admissibility of electronic records in litigations, they tend to approach this topic primarily from two perspectives: 1) identifying gaps in the law and in the records and archives management processes that hinder the admissibility of electronic records as evidence in legal proceedings, and proposing improvements to address these gaps,[29] and 2) identifying the provisions relevant to records and archives management on the basis of which requirements for the management of electronic records that would improve their admissibility can be developed.[30]

Some legal gaps identified by Chinese scholars as inhibiting the admissibility of electronic records relate to existing provisions on the legal effectiveness of electronic records, the rules governing the admission of electronic records, the applicability of the best evidence rule to electronic records, and the assessment of the authenticity of electronic records.[31] The records and archives management issues that inhibit the admissibility of electronic records include: lack of a coherent set of general requirements, specifications, and standards guiding the management of electronic records; conflicts in administrative control over the management of electronic records; ineffective measures for the management of metadata; weak security; and an absence of technologies designed for the management of electronic records.[32] More recently, Chinese scholars have started comparing the meaning of authenticity in the fields of law and archival science[33] and scholars in the legal field are acquiring familiarity with the archival field and have published papers in archival journals comparing the rules of admissibility (i.e.,

authenticity, relevance, and legality) and probative force with the concepts of authenticity, reliability, and usability of digital records as discussed in the archival field.[34] Chinese scholars recognise that it is the records managers and archivists' responsibility to guarantee to the fullest extent and by means of management measures the authenticity of electronic records.[35]

While there is growing research on the evidentiary capacity of electronic records in the archival field, collaborations between experts in evidence law and archival science are rare.[36] Few of the writings approach the admissibility of electronic records systematically from the point of view of the rules governing it;[37] what's more, the examination of the rules is cursory rather than thorough and substantial.[38] These gaps in the existing literature make the present study necessary and unique. In addition, most archival publications in English on the admissibility of electronic records as evidence are written from the common law perspective, rather than from the perspective of China's civil law system.

Challenges for the admission of digital records as evidence in civil cases in China

The Chinese legal system

The Chinese evidence system was deeply influenced by the law-making tradition of Japan and the Continental Europe Legal System.[39] As opposed to the adversarial system adopted in common law system, the Chinese legal system is an inquisitorial system, the prevailing system in civil law jurisdictions, including continental Europe and Latin America; under it, 'the court plays an active, authoritative, and interventionist role at all stages of the proceedings, while the parties have only a minor, tentative, and supportive function.'[40] For instance, a judge in China can investigate and collect evidence either per request of the parties or when it is deemed necessary by the judge for finding the truth; the aim is 'to remedy the deficiency of the competency of parties in collecting evidence and help fact-finders to make factual determination accurately.'[41]

Furthermore, while the admission of evidence in adversarial systems is usually determined by the judge based on rules, the acceptance and rejection of evidence, as well as its probative force, in China, are primarily based on the judge's conscience and rationale,[42] with rules taking on an auxiliary role. For instance, the 2019 revision of *Some Provisions on Evidence in Civil Procedures* prescribes that:[43]

> Article 85. The judges shall verify the evidences according to the legal procedures all-roundly and objectively, shall observe the provisions of law, follow the professional ethics of judges, use logical reasoning and daily life experience to make independent judgments concerning the validity and forcefulness of the evidences, and publicise the reasons and result of judgment.

In addition to the principle adopted for examining evidence, the nature of truth that is sought in fact-finding also varies between the inquisitorial system and the adversarial system: namely, the former is an objective truth and the latter a legal truth. The inquisitorial system as associated with the Chinese legal system usually seeks facts at the ontological level and requires that 'people involved in judicial activities should make their cognitive facts completely tally with the ontological facts,' viz., the objective truth.[44]

The adversarial system usually seeks truth constructed based on the evidence available and what the law describes or admits, viz., the legal truth.[45]

Paper and digital records as two separate types of evidence

In the common law context, evidence is usually divided into four categories: oral evidence, documentary evidence, real evidence, and demonstrative evidence;[46] records in any form are categorised as documentary evidence. In China, pursuant to Article 50 of the *Criminal Procedure Law of the People's Republic of China (2018 Amendment)*, all materials that may be used to prove the facts of a case are considered as evidence. Further, the three major procedural laws identify and enumerate the types of evidence[47] that can be used in litigations,[48] including, for instance, statement of a party, documentary evidence, physical evidence, audio-visual recordings, electronic data, witness testimony, expert opinion, and transcripts of survey, types that are substantially the same as those listed in common law, but more useful to the Chinese practice.[49]

As per the categorisation stipulated by the three procedural laws, when paper records are identified as a type of documentary evidence, digital records are identified as a type of electronic data evidence.[50] Therefore, paper and digital records belong to two different categories of evidence. The de facto separation of paper and digital records in two different categories of evidence in procedural laws may lead to the perception that rules for the admission of paper records are not relevant to the admission of digital records and, as a result, may cause incongruity in the management of paper and digital records in organisations.

Rules governing the admission of paper records

Paper records or records in paper form are identified as a type of documentary evidence in the three procedural laws in China, which, according to the *Provisions on Uniform Evidence in People's Courts (Proposed Draft for Judicial Interpretation)*,[51] refers to records that contain information regarding the facts in the case in writing – such as words, number, or graphs – and recorded in paper. This definition of documentary evidence in China is substantially equivalent to the Canadian definition: 'recorded information admitted as evidence in legal proceedings'[52] except for the fact that documentary evidence in China is restricted to documents on paper.

In the common law system, the rules governing the admission of documentary evidence are besides relevance, authentication, best evidence, and the business records exception to the hearsay rule.[53] The authentication of a record submitted as evidence (i.e., the attestation of its identity) and the application of the best evidence rule (i.e., the presentation of the original or, in its absence, of the most authoritative copy, to support the demonstration of integrity) address the authenticity[54] of the record (i.e., the record is what it purports to be and is free from tampering or corruption), while the exception to the hearsay rule also deals with the reliability of records (i.e., the trustworthiness of the statement contained within the record).[55]

In China, the three major rules governing the admission of documentary evidence are relevance, legality, and authenticity. Under Article 67 of the *Civil Procedure Law of the People's Republic of China (2017 Revision)* (hereafter 'The Civil Procedure Law'), 'a

people's court shall identify the authenticity and examine and determine the validity of documentary evidence provided by the relevant entities and individuals'. The Civil Procedure Law does not provide further explanation as to what 'authenticity' and 'validity' refer to in this clause. Yet, Chinese law scholars contend that the purpose of this article is to guarantee the 'formalistic authenticity'[56] and 'material authenticity'[57] of the records produced as evidence in court,[58] with the former referring to whether the record has been corrupted or tampered with,[59] and the latter referring to the consistency between what is recorded in the content of the record and the fact to be proven.[60] In addition, it is required that 'the original of documentary evidence shall be submitted', which is consistent with the spirit of the best evidence rule in the common law context. Additionally, *Provisions on Several Issues Concerning the Examination and Judgement of Evidence in Death Sentence Cases* confirms the employment of these three rules in the examination of documentary evidence, as stated in Article 6 below,

> Article 6. The examination of physical or documentary evidence shall focus on:
>
> Whether the physical or documentary evidence is the original object or document, and whether the photos, visual recordings or the reproductions of the physical evidence or the duplicates or photocopies of the documentary evidence are identical with the originals [the best evidence rule]; whether the physical or documentary evidence has been identified [the authentication rule], authenticated [the exception to hearsay rule]; whether the photos, visual recordings or the reproductions of the physical evidence or the duplicates or photocopies of the documentary evidence are made by two persons or more, and whether there is any written explanation and signature of the makers regarding the process of making reproductions and the place where the original object or document is put [the best evidence rule].

While Chinese laws have hinted to the use of these three rules governing the examination of documentary evidence for its admissibility as evidence, the lack of specific criteria and guidelines in legislation and legal cases, and the prevalence of the judge's conscience and rationale in the examination of the evidence make the application of these rules in judicial practices rather vague and ambiguous.[61]

For instance, provisions specifically dedicated to the authentication of documentary evidence in Chinese legislations are scant. Furthermore, authenticity of documentary evidence is not treated and examined independently based on a set of specifications, but is inferred from the fact that the documentary evidence is original. As a result, the authentication rule does not enjoy an independent status as its counterpart in the common law world, but is embedded into the submission of originals rule. See Article 94 of the *Provisions on Uniform Evidence in People's Courts (Proposed Draft for Judicial Interpretation)*:

> Identification refers to creator, collector, keeper, and other witnesses that have personal knowledge of the physical evidence, documentary evidence, and demonstration evidence identify their source and chain of custody, including:
>
> (1) whether the evidence is relevant to the facts in the case, and whether it is sufficient to support the adducing party's claims;
>
> (2) whether the evidence is the original object or document;

> (3) whether the reproductions of the physical evidence or the duplicates of the documentary evidence are identical with the originals; and
>
> (4) whether the evidence has maintained its original properties and whether it has been tampered with or modified.

This Article identifies three aspects to be focused on when performing identification: relevancy, whether the evidence is original, and whether the reproduction of the evidence is identical to the original. These three aspects should be determined on the basis of the source and chain of custody of the submitted evidence. The recognition of the impact the source and chain of custody of the evidence have on its authenticity is crucial in that it recognises that the essence of authenticity is about what has happened to the evidence after its creation. Yet, further information is needed to clarify what requirements should the source and chain of custody of the evidence satisfy for it to be considered as authentic.

The best evidence rule concerns the preference for originals of evidence and under what circumstances reproductions of the originals can be submitted as evidence. For instance, under Article 61 of the *Some Provisions on Evidence in Civil Procedures (2019 Amendment)*, it is stated that:

> Article 61. During the cross-examination of documentary evidence, physical evidence and audio-visual recordings, the parties shall produce the original evidence or the original, except under the following circumstances:
>
> (1) The original evidence or the original is compellingly difficult to produce, and the people's court grants the producing of a copy or reproduction; and
>
> (2) The original evidence or the original no longer exists and evidence shows that the copy or reproduction is consistent with the original evidence or the original.

As to the examination of the trustworthiness of statements contained within the record (the Chinese counterpart of the exception to hearsay rule), Article 114 of *Interpretation of the Supreme People's Court on the Application of the Civil Procedure Law of the People's Republic of China*[62] specifies the presumption of reliability of public records created by a state agency and other public organisations. However, these documents are all public. Article 97 of *Provisions on Uniform Evidence in People's Courts (Proposed Draft Judicial Interpretation)* provides some guidance on the examination of the authenticity and reliability of private records focusing on the creation and maintenance of records. Yet, further specification in terms of what criteria should the author, source, content, place of maintenance of the records satisfy for the records to be considered reliable and authentic is needed to assist the examination.

Additionally, according to the Civil Procedure Law, 'A party shall have the burden to provide evidence for its claims'.[63] And while there is discovery[64] in civil litigation in the common law world, it was only in 2015 that *Interpretations of the Supreme People's Court on the Application of the Civil Procedure Law of the People's Republic of China* stipulated that a party can, with the assistance of the court, request the opposing party to submit the documentary evidence that is under its control (Article 112). Prior to the introduction of this Article in 2015, in civil litigations, a party could only submit documentary evidence that was under its control or under the control of a third party, and it was very easy for the opposing party to dispute the reliability and authenticity of evidence submitted under

the control of the submitting party, considering the motivation to do so. When such disputes arise, the court has to decide whether the burden of proof of the reliability and authenticity of the submitted evidence should fall on the submitting party or the opposing party; judicial practices show that judges are not consistent with this.[65] Either way, the lack of guidance and criteria for proving the authenticity and reliability of documentary evidence makes it considerably hard to do it.

While rules governing the admissibility of private records in Chinese civil litigations are equivalent to those in the common law world, the lack of specific guidance on the application of these rules makes it hard to implement them in practice. This is further complicated by the principle of burden of proof and the prevalence of logical reasoning and daily life experience when the judges evaluate the evidence.

Rules governing the admission of digital records

Research on electronic evidence in the Chinese legal field commenced in the 1980s,[66] and has been ongoing since. The enactment of the *Contract Law of the People's Republic of China*[67] in 1999 and the *Electronic Signature Law of the People's Republic of China*[68] in 2005 endowed electronic data with legal effects, and hence, officially approved the use of electronic data in the conduct of business. Yet, it was only with the addition of electronic data as a type of evidence in the three major procedural laws that the ability of electronic data to be used as evidence in litigations was legally recognised. However, other than recognising electronic data as one type of evidence to be used, the three procedural laws do not specify rules for electronic data collection, storage, transfer, display, or examination, or the probative force of electronic data in judicial practice.

Recently, three judicial interpretations for criminal cases have specified procedures and rules for the collection and display of electronic data evidence. The three major rules – relevance, legality, and authenticity – apply to the admission of electronic data as well. And the focus here is on authenticity. For instance, *the Provisions on Several Issues Concerning the Examination and Judgement of Evidence in Death Sentences Cases*[69] stipulates the use of the following rules in the examination of electronic evidence: (1) a hardcopy of the electronic evidence has to be submitted together with the electronic evidence; (2) relevancy; (3) authenticity; (4) use of forensic examination when there is doubt about the electronic evidence; and (5) examination of electronic evidence in combination with other evidence.[70]

The Provisions on Several Issues Concerning the Collection, Taking, Examination, and Judgement of Electronic Data in the Handling of Criminal Cases,[71] issued in 2016, outlines the collection and taking, transfer and display, and examination and evaluation of electronic evidence in criminal cases, and its primary goal is to protect and demonstrate the integrity of electronic data in the process. Therefore, for instance, examination of the authenticity of electronic data focuses on the following aspects: (1) whether the original storage medium is transferred and if not, whether explanation is provided as to why and the process of collection and taking; (2) whether electronic data have special identifiers such as a digital signature and a digital certificate; (3) whether the process of collecting or taking electronic data may be replayed; (4) whether an explanation is attached where electronic data are added, deleted, or modified; and (5) whether the integrity of electronic data may be guaranteed. Then, in 2019, *the Rules of Obtainment of Electronic Data as*

Evidence by Public Security Authorities in Handling Criminal Cases[72] regulated the implementation of different methods used in the collection and taking of electronic data, examination and investigative re-enactment of electronic data, as well as its commissioned inspection and appraisal.

The aim of these three documents is to regulate the process for the collection, preservation, and display of electronic data so that their evidentiary capacities will not be questioned by the accused in prosecution. Since it is investigation officials who carry out the collection of evidence in Chinese criminal cases, it is presumed that, as long as the identity and integrity of the electronic data during its collection, transfer, and presentation – hence, its authenticity – can be protected, the electronic data will be admitted in court as evidence.

In comparison with criminal cases, the admission and the examination of electronic evidence in civil cases are more complicated and face more challenges. There were no specific rules for the examination of electronic evidence in civil cases until September 2018, when the *Provisions of the Supreme People's Court on Several Issues Concerning the Trial of Cases by Internet Courts* was issued.[73] Article 11 of this judicial interpretation on the Trial of Cases by Internet Courts stipulates how to examine the authenticity of electronic data when disputes arise, focusing specifically on, for instance, reliability of the computer systems, storage media, and extraction and fixity methods of electronic data, etc. In addition, Article 11 also requires that electronic data whose collection, fixity, or protection utilises technologies such as electronic signature, trusted time stamp, hash value check, or blockchain, or which are certificated by an evidence collection or preservation platform, should be confirmed by the court, provided that their authenticity can be proved, as follows:

> The Internet court shall confirm the electronic data submitted by the party concerned through electronic signature, trusted time stamp, hash value check, blockchain or any other evidence collection, fixation or tamper-proofing technological means, or through the certification by an electronic evidence collection and preservation platform, provided that the authenticity of the electronic data can be proved.

Recognition of the capabilities of technologies such as trusted time stamp and blockchain, and evidence collection and preservation platforms in protecting electronic data's integrity may encourage their use in the collection, fixity, and submission of electronic data in legal proceedings.

In December 2019, *Some Provisions of the Supreme People's Court on Evidence in Civil Procedures* were revised and clauses were added on definition and examination of electronic data in civil cases. Article 93 stipulates a list of factors to be considered in the examination of the authenticity of electronic data, which can be organised into the following four categories: (1) soundness and reliability of the computer system's hardware and software environment in which the electronic data are generated, stored, and transmitted; (2) reliability of methods used for the preservation, transmission, and retrieval of electronic data; (3) evidence that the data is generated and stored in the usual and ordinary course of business; and (4) evidence that the party storing, transmitting, and retrieving the electronic data is appropriate.

A comparison of these requirements with the rules governing the admission of electronic records in common law countries shows that there are overlaps between

them. The underlying rationales for them are that the integrity of a system guarantees the authenticity of the records stored in it and that the 'nature of bureaucracy', 'the mercantile nature of record', or the systematic and habitual nature of the creation of records in the ordinary course of business can guarantee this.[74] Yet, because this interpretation is very recent, there are few legal cases to investigate how these rules are applied in the Chinese context in practice.

In addition to identifying a list of factors to be considered in the examination of electronic data, the Provisions on Evidence in Civil Procedures also stipulates a list of circumstances wherein the authenticity of electronic data can be presumed unless otherwise proved by sufficient evidence to the contrary. These include:

> (1) wherein a party submitting and keeping electronic data that is unfavourable to it; (2) wherein the electronic data is provided or confirmed by a neutral third party platform that records or keeps the data; (3) wherein the electronic data is created in the usual business activities; (4) wherein the electronic data is kept by means of archive management; and (5) wherein the electronic data is stored, transmitted, and retrieved by means agreed by the parties (Article 94).

The third circumstance also seems to be one of the factors to be considered in the examination of electronic data's authenticity as discussed above. This is very confusing, because, as on one hand, electronic data created in the usual business activities are presumed to be authentic, yet, on the other hand, this is only one of the factors considered in assessing electronic data's authenticity.

The fourth circumstance that electronic data kept by means of archive management can be used to justify the value of records and archival management program in guaranteeing the evidentiary capacity of electronic data in organisations. Yet, this statement is quite general and does not specify what 'by means of archive management' involves. In other words, can electronic data managed by poor archival management program still be presumed authentic?

At the moment, there is no ongoing discussion either in the legal field or the archival field on the implications and influences of the third or fourth circumstances: no legal cases are identified referencing them in assessing the authenticity of electronic data submitted as evidence. In contrast, the second circumstance, concerning the use of a neutral third party in evidence preservation attracted much attention even before the enactment of this judicial interpretation.

The use of a third party for evidence collection and preservation

Chinese judicial practice shows that electronic evidence is less often used in civil cases than in criminal cases[75] to the extent that electronic evidence is basically marginalised in civil cases and stands in an 'awkward position'.[76] Part of the reason is the principle of the burden of proof in Chinese litigations which prescribes that a party shall have the burden to provide evidence for its claims according to the procedural law of civil cases,[77] and that, because the discovery process in China is different from that in the United States,[78] the plaintiff or defendant mostly submit electronic evidence that the party or a third party has maintained or controlled.[79] Owing to the fact that electronic evidence is easy to corrupt and the party has motive to do so in order to support its claims, electronic evidence under the control of a party is easily challenged by the opposing party.[80]

Additionally, prior to the enactment of the 2019 revision of *Some Provisions of the Supreme People's Court on Evidence in Civil Procedures*, there were no clear rules and principles guiding the examination and determination of the electronic data submitted as evidence in legal proceedings.[81] Thus, the parties have to use other approaches to prove the reliability and authenticity of the electronic data submitted as evidence in civil cases. These approaches include:[82] printing out the digital evidence and submitting the paper printout in its place;[83] asking a notary or copyright society to collect and preserve the digital evidence;[84] asking the court to collect and preserve the digital evidence;[85] and asking a third party to preserve the evidence. The first three approaches are established and traditionally commonly used for evidence preservation. Yet, they have presented several issues. For instance, authenticity of the paper printout is easily challenged by the opposing party during the cross-examination stage and hard to prove, considering that the electronic data is easy to tamper with and destroy.[86] Use of a notary service usually takes too long and the evidence may have already disappeared; in addition, it is expensive and the notary service may not have the technologies required.[87] These limitations led to the introduction of use of a third party for evidence collection and preservation, which, as argued, will become the new 'normal'.[88]

According to Li, Zizhu, a judge at the Intellectual Property Court of the Supreme People's Court electronic evidence preservation by a third party means that

> A party uses a third party electronic evidence platform to collect and preserve existing electronic evidence or electronic evidence that is in the process of generation. Or per the request of the party, the third party electronic evidence platform collects and preserves existing evidence or electronic evidence that is in the process of generation on behalf of the party. The purpose is to ensure that evidence collected and preserved will not be tampered with, its integrity maintained, and the time for collection and preservation confirmed.[89]

Third-party evidence platforms are profit-based companies independent of the parties in litigation and specialising in the provision of evidence collection and preservation services.[90] For this reason, they are usually considered neutral.

The first third-party evidence preservation company in China was established in 2008, but afterwards, the industry developed very slowly; then, since 2015, the industry has experienced explosive growth.[91] According to an industry report, in 2018, the electronic data forensics market in China was valued at approximate RMB 1.8 billion and it was predicted that in 2023, the market will be valued at about RMB 3.6 billion; further, while the primary customer groups of electronic data forensics business are judicial and administrative law enforcement departments, the customer base has been expanded to enterprises.[92] Studies also show that the number of legal cases involving third-party evidence collection and preservation is increasing rapidly.[93]

In contrast to the rapid development of the third-party evidence collection and preservation industry, academic studies on this approach are few[94] and emerged only recently. Most of these studies have explored existing issues with this approach and proposed strategies to address them. They relate, for instance, to the probative force of evidence collected and preserved by the third party,[95] the lack of clear guidelines on the qualifications of the third party,[96] the absence of standards and regulations on the technologies and processes used for the collection and preservation of evidence,[97] and

the authenticity of the evidence prior to its collection and preservation,[98] all of which raise concerns about authenticity of the evidence collected and preserved by a third party.

There is no standard or model for third-party evidence collection and preservation. Methods and technologies used vary across different service providers, and depending on the types of electronic data to be collected, whether collection occurs prior to or after the creation of the data, and whether the collection is performed online or offline. For instance, for the collection of a website containing infringing material by using the trusted time stamp service provided by the UniTrust Time Stamp Authority,[99] the steps involved are: (1) registering as a user on the service provider's website and then logging into the evidence collection system; (2) enabling the screen recorder function provided by the computer to record the process and at the same time using an external video recording device to record the whole operation; (3) running a full computer scan to make sure there is no virus, cache is cleared, etc.; (4) fixing the evidence by going to the infringing website, taking a screenshot of the webpage containing infringing material, checking the ICP (Internet Content Provider) licence, requesting time stamp for the screenshots of the webpage, requesting time stamp for the video recorded.[100] There are also services that are offering one-stop solution whereby the users simply need to provide the webpage that they want to collect and preserve and the service will automatically perform the collection and preservation activities.

Technologies commonly used by third-party platforms for protecting the electronic data's authenticity include digital signature, blockchain, trusted time stamp, encrypted transmission, and hash value check. Cloud service is also used for the storage of the electronic evidence collected and preserved. Some services are also collaborating with the notary service, on one hand, to increase their credibility, and on the other hand, to add another 'chain' to ensure the security of the electronic data.[101] Usually, the third-party platform will work together with the notary service and once collection and preservation for certain electronic data are finished, the third-party platform will transfer related documents and a description of the process to the notary service, whose system will assess the preservation based on certain algorithms and provide certification; no human is involved in the process.[102] It appears that, at the moment, third-party platforms purely rely on technological approach for the maintenance of the electronic data's integrity.

Despite its popularity, this approach is not without drawbacks and limitations, and not all evidence collected and preserved by a third-party platform can be admitted in a court of law. A recent study of 100 legal cases using a third-party platform for evidence collection and preservation shows that 24 cases were not admitted.[103] The reasons the courts gave for the rejection of the evidence collected and preserved by a third party include: (1) evidence collection and preservation by a third party was identified by the court as certification by notary service; yet, notary requirements were not satisfied; (2) there were no originals to compare the evidence to; (3) the qualifications of the third-party platforms were in doubt; and (4) the reliability of the preservation methods was in doubt.[104]

While collection of electronic data by a third-party platform can occur simultaneously with their creation, it may also occur after their creation. Especially when the party itself uses the tool provided by the third-party platform to perform data collection, it is possible that the data uploaded are inauthentic. And even when it is the third-party platform itself that performs the collection, the later the collection takes place, the more

likely it is that the environment where the electronic data reside becomes contaminated. In other words, the third-party platform can at most protect and prove the integrity of the data when it is in its custody; it cannot prove its integrity prior to its collection. Therefore, it is argued that electronic data collection should be performed early in the life of the records, at a time when the authenticity of the electronic data can be guaranteed.[105] From an archival perspective, however, unless collection occurs simultaneously with the creation of the electronic data, merely advancing the collection to a time closer to the creation cannot guarantee the authenticity of the electronic data to be collected.

Other concerns mainly revolve around whether the authenticity of electronic data in the third-party platform can be ensured. This concern arises from two issues: the reliability of the third party and the reliability of the methods and technologies used by the third party;[106] the former regards the neutral role of the third party and the latter regards the capacity of the technologies used. For the former, how to make sure the third party is truly independent of the parties in litigation and that it will not tamper with the data for the interest of either party, is critical.[107] For the latter, whether the technologies used can fully guarantee the integrity of the electronic data and whether there is a possibility that the data be compromised are serious questions. Taking the use of blockchain technology as an example, at the moment, because most services based on blockchain are concerned about the authority and national credibility of the 'chain', the number of chains is not high and mostly include the court, the prosecutor, the notaries, forensic centre, and others connected offices. However, strong credibility of the chains does not necessarily indicate high security of their computer systems, therefore, theoretically, there is a high risk of attacks.[108]

Further, while the judicial interpretation on the Trial of Cases by Internet Courts still require the authenticity of electronic data preserved by a third-party platform to be proved, the Provisions on Evidence in Civil Procedures simply state this evidence can be presumed authentic unless there is sufficient evidence to the contrary. Does this mean that the court will not perform an examination of this evidence? As evidence collection and preservation by a third party is increasingly used by individuals and enterprises so as to improve admissibility in legal proceedings, it is critical that the identified drawbacks and limitations be addressed and robustness of the process improved.

ITrust PaaST: enhancing the third-party approach for the protection and demonstration of the authenticity of electronic data

As discussed, promoting the digital transition in China requires that the evidentiary capacity of digital records be protected and demonstrated so that they can be used to demonstrate, in the course of regular audits or inspections, that an organisation has met legal, regulatory, and fiscal requirements, or to protect its interests in resolving legal disputes, especially for the private sector. To protect and demonstrate the evidentiary capacity of digital records (i.e., electronic data in China) in a court of law, it is necessary that the records and archives management field and the legal and law enforcement field collaborate.

The above review of the Chinese legal system, legislations and judicial interpretations relating to the admissibility of electronic data in civil cases shows that the collaboration between the legal field and the records and archives management field may not be easy.

Yet, there are good signs: for instance, the statement that electronic data managed 'by means of archive management can be presumed authentic is favourable to the archival field. In recent years, writings in the Chinese records and archival field on the evidentiary capacity has increased; however, discussion of how archival knowledge can contribute to addressing issues in the legal field have not gone very far. This section will discuss how the PaaST model can be used to enhance the third-party approach that is popularly used for evidence collection and preservation in China.

The Preservation as a Service for Trust (PaaST) model is a set of functional and data requirements for digital preservation developed by the InterPARES Trust (Hereafter ITrust) project.[109] Its development was prompted, in part, by the challenges posed to digital preservation by the use of cloud-based services, more specifically, 'the loss of control over, and even knowledge of, what hardware and software are used and how they are used [in the preservation of digital information]';[110] by the vision of what trustworthy preservation systems will look like in the future, given that more and more computing resources and services are delivered as a service;[111] and by the diversity in the preservation environments, for instance, the variety of the objects to be preserved, the information systems involved, the requirements for preservation, and the institutional arrangements and relationships among the parties involved, etc. Thus, the model is intended to 'support as broad a range of situations as possible, including differences in what is being preserved, the objectives of preservation, the policies that govern preservation, who is involved in what capacity and even, to some extent, how preservation is accomplished.'[112]

The ITrust PaaST model builds on the findings and recommendations of the three preceding InterPARES projects and the ISO Open Archival Information System (OAIS) standard.[113] The OAIS model provides some concepts and requirements for the PaaST model[114]; yet, new classes of objects were also introduced and existing ones were refined. For instance, the PaaST model introduces six capacities driven by the assumption that preservation activities may be performed by agents with different responsibilities.[115] Further, the PaaST model differs from the OAIS reference model in that (1) it only focuses on information objects that are digitally encoded, thus excluding records in paper format, (2) it only includes functionalities that are specific to preservation, and (3) it does not envision a coherent system for preservation but expects that the capabilities may be distributed among a range of service providers. In addition, aiming to be directly implementable, the model is articulated in Unified Modelling Language (UML) and has restricted its scope only to those functionalities that are implementable in computer systems. The model is intended to be technology neutral and does not prescribe what technologies should be used to deliver the services required.

The use of the term 'as-a-service' in the name of the model indicates that its implementation will enable digital objects to be preserved in an authentic manner: what is retrieved is identical to what had been ingested or, if there are changes, there is sufficient evidence to demonstrate that the differences will not affect the ability of the digital objects to serve whatever purpose they are intended for,[116] regardless of what technologies, methods, or tools have been used to accomplish this. Thus, the model allows the execution of different preservation actions in accordance with the characteristics of the digital objects and the requirements for preservation. For instance, instead of a preservation system, the PaaST model introduces the concept of 'Preservation

Environment' to describe the objects that are kept under the same preservation requirements, and the technological infrastructure and tools used to perform preservation. The model is intended to accommodate preservation performed in an in-house environment, a cloud environment, or a combination of both.

The essential components of the model include: 1) digital objects to be preserved and their significant properties whose persistence is essential to verify the success of the preservation; 2) preservation actions to be performed to make sure that digital objects remain authentic, accessible, and usable in the course of technical upgrade, obsolescence, reuse, etc.; and 3) preservation management information, which includes information on the digital objects to be preserved, the preservation actions taken with respect to the digital objects, and the outcome of the preservation actions. Figure 1 presents an overview of the central classes involved and the relationships among them.

While the OAIS model defines three roles, which are Producer, Consumer, and Management, the PaaST model makes further differentiation of the roles involved or capacities a person, organisation, external system or application interacting with a Preservation Environment may have and defines six capacities. On the supply side, PaaST differentiates between the person or entity that created or originally owned or controlled the digital objects (i.e., Producer), the person or entity that has possession of and/or control over digital objects and has authority to decide or agree to what is to be preserved and the terms under which they will be preserved (i.e., Initial Source), and the person or entity that sends digital objects and related information to a Preservation Environment (i.e., Submitter). On the demand side, there is the capacity of Access Client, that of Preservation Director, which decides the actions that are to be executed and by whom, and evaluates the results; and that of Preservation Service Provider, the party that provides technological capabilities and services to carry out preservation.

A class of Actor is also defined as a role of some entity that is relevant to the specification of its associated use cases. The four predefined roles an Actor may perform in implementing PaaST requirements include Performer,[117] Authoriser,[118] Problem Resolver,[119] and Approver.[120]

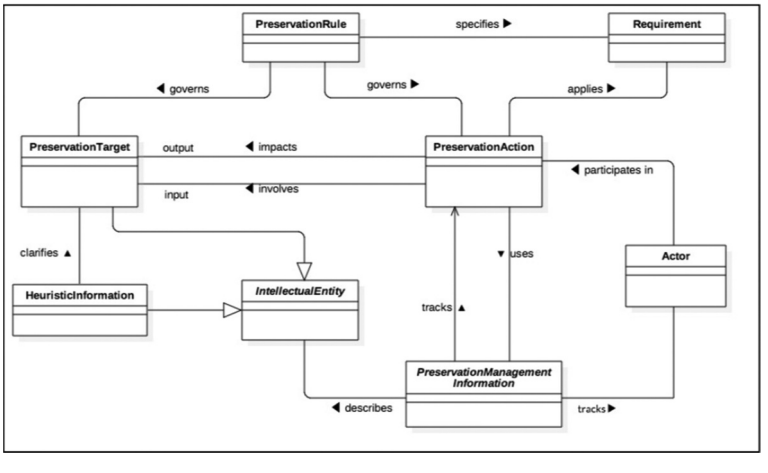

Figure 1. Preservation overview.[121] Taken from Thibodeau et al., p. 15.

The digital objects that are to be preserved are identified in the model as *preservation targets*, some of whose features must be qualified explicitly as *permanent features*, that is, features which should remain invariant regardless of changes in *binary encodings* of the *preservation target*, or in technologies used to carry out preservation.[122] Any feature of a *preservation target* can be identified as *permanent feature* depending on the purpose and requirements of the preservation. The focus of verification as to whether the preservation has been successfully performed is the expression of these *permanent features*, which are usually described in three facets: existence, value, and the manner in which they are expressed. This focus on the properties of digital objects whose persistence is essential to evaluate the success of preservation reflects the objective of the model to preserve the information that is digitally encoded rather than the technology that is used for preservation. *Preservation targets* and *Heuristic information*[123] are two specialisations of the general class *Intellectual entity*.[124] The two central classes *Requirement* and *Preservation rule* are preservation norms that control what is preserved, what actions are performed and the conditions that govern them.

Actions to be performed to accomplish preservation include: 1) transferring and ingesting *preservation targets* into a Preservation Environment; 2) managing the storage of the *preservation targets* to ensure that they can be instantiated with all *permanent features* unchanged; 3) producing a new *binary encoding* of the *preservation targets* and ensuring that the change and process comply with preservation objectives and requirements; 4) accessing *preservation targets* and other capabilities, such as preservation actions, preservation management information, etc.; and 5) verifying that the preservation is successful with regard to the intended use of the digital objects.

In order to 'support as broad a range of situations as possible', the PaaST model allows customisation and specification of the digital objects and the preservation requirements in accordance with the characteristics of the *preservation targets*, the objectives of preservation, and the preservation environments. For instance, the digital objects to be preserved and all information involved in carrying out preservation are organised in a taxonomy of classes at general levels, which can be specified with more precise subclasses. All preservation requirements are organised into groups of related capabilities that can be added, selected, or supplemented by breaking down each requirement into more specific ones that are appropriate for different situations. Further, the model allows 'both the allocation of different preservation tasks to different agents and the execution of these tasks, by one or more agents, using different methods and … potentially unrelated technologies, under separate and independent administrative or operational control.'[125] At the most general level, the *Preservation Environment* can involve a variety of entities, which can be either in-house or in the cloud, each taking responsibility for part of the digital preservation function. In addition, one building block of the PaaST model is 'knowledge that any changes in storage, encoding, or the technologies used to process the data have neither corrupted the preservation objects nor impeded the possibility for rendering the data objects appropriately'.[126] This knowledge and the documentation of this knowledge can help demonstrate the authenticity of the information objects submitted.

The PaaST model can be used by the third-party platform for the preservation and verification of the evidence it collects and preserves, specifically for addressing the issues concerning the neutral role of the third party and the reliability of the methods it used for

protecting the integrity of the electronic data. A core concept underlying the PaaST model is the 'black box' processes, meaning 'what matters are not the internal components of the process used in preservation, but whether the output faithfully reproduces the input'.[127] This is consistent with the expectation of the use of a third-party approach for evidence collection and preservation, in that the parties do not care about the methods and technologies used, as long as the evidence submitted and/or collected by the platform can be reproduced in such a way that its integrity can be confirmed by the court.

At the moment, a variety of technologies are used in the preservation of the evidence collected by the third-party platform and for the demonstration of its integrity. These technologies usually involve the knowledge of computer science, cryptography, etc.; thus, they are not intuitive to most people; when the opposing parties do not understand the technologies, they are more likely to deny the evidence.[128] In addition, there is a lack of clear explanation by the evidence-submitting party regarding the source of the electronic data evidence, its generation, and the preservation methods used, and this will pose difficulties for the examination of the authenticity of the evidence by the court.[129]

The PaaST model can help address this issue by supplementing the use of technologies with a description of the electronic data, showing that those reproduced and presented to the court are the same as those provided to the third party by the party submitting evidence, and demonstrating what preservation activities have been performed on the electronic data evidence and by whom. The PaaST model is applicable to the third-party evidence preservation scenario by customising the taxonomy of classes to reflect its purpose.

Conclusion

Technological context is one major force that has influenced the records and archives field over the past two decades and the archival discipline has to contemplate and address the influence of and challenges raised by information technology as an object of study and theory and methods development. This article shows that, while the choice of methods required to address the challenges brought about by digital technology are usually influenced by the legal, regulatory, and other aspects of each juridical-administrative system, as well as by recordkeeping and archival traditions, archival knowledge remains valid across contexts and can develop universal solutions. Thus far, the voice of the Chinese records and archival field has been quite weak with regard to the protection and demonstration of the evidentiary capacity of electronic data. But the international field, collaborating across disciplines, has been able to develop ways of addressing these issues that are compatible with the Chinese juridical-administrative system. This article shows the relevance and potential of the PaaST model for addressing some of the issues on the third-party approach for electronic evidence collection and preservation in China. Given the opportunities presented by the *Some Provisions of the Supreme People's Court on Evidence in Civil Procedures*, the Chinese archival field may want to seize this opportunity to demonstrate its relevance in the digital era.

Notes

1. The Chinese original is 电子文件归档与电子档案管理研究领导小组.

2. Huiling Feng, 走向单轨制电子文件管理['Towards Single track system of Electronic Records Management'], *Archives Science Study*, no. 1, 2019, pp. 88–94.
3. The terms electronic and digital are used in this article to refer respectively to the method of transmission of the records (which are carried by an electrical conductor and requires the use of electronic equipment to be intelligible by a person) and to their form (which is represented through discrete, binary values).
4. Feng.
5. Weimei Pan, Guan Jiang, Yajing Ji, and Zhiying Liu, 'Survey on Needs of Users of Archival Outsourcing Services', Unpublished report.
6. Feng.
7. Jizong Liu, 企业档案双套制保管的'囚徒困境'及最佳出路 ['The prisoners' dilemma in the use of dual-copy system in enterprise archives management and the best responding strategy'], *China Archives*, no. 11, 2015, pp. 56–59.
8. Yan Chen,'双套制''双轨制'走向何方['What are the future directions for the dual-track system and the dual-copy system?'], 机电兵船档案, no. 2, 2018, pp. 36–38; Shuilong Tao and Lei Tian, 电子档案双套制管理问题研究 ['On the double-sets management system of electronic archives'], *Archives Science Study*, no. 4, 2014, pp. 61–64.
9. Huiling Feng, 电子文件与纸质文件管理的共存与互动 ['The co-existence of and interaction between the management of electronic records and paper records'], *China Archives*, no. 12, 2003, pp. 40–42; Hongwei Liu,'双套制'与'双轨制'对电子文件管理的影响 ['The influence of "the dual-copy system" and "dual-track system" on electronic records management'], *Archives Management*, no. 5, 2011 pp. 20–22; Qianqian Yang, 我国文件档案'双轨制'管理模式转型 – 澳大利亚政府数字转型政策的启示 ['Transition of dual-track system in records and archives management of China: Enlightenment of Australian government's digital transition policy'], *Archives Science Study*, no. 3, 2014, pp. 9–13.
10. Bing Li, 对电子文件'双套制'归档含义的理解 – 同一份文件的两种版本与两个部分 ['An interpretation of the dual-copy system – One record's two versions or two parts'], *China Archives*, no. 9, 2011, pp. 32–33.
11. Feng, 'The co-existence of and interaction'; Tao and Tian.
12. For instance, in the *Specification on Electronic Documents Archiving and Electronic Records Management* (GB/T 18894–2002), it was required that, if textual and graphical digital records identified as having long-term preservation value have no paper copies, a paper or microfilm copy has to be generated, and both have to be kept (Article 4.5). In *Measures on Filing and Transferring of Records at State-Owned Enterprises*, issued in 2004, it was stipulated that, for digital records identified as having permanent or long-term preservation value, a paper copy had to be generated and transferred (Article 21). And, in *Interim Measures for the Administration of Electronic Documents*, issued in 2009, it was required that for digital records identified as having permanent preservation value or other important value, a paper or microfilm copy has to be generated and transferred (Article 16).
13. Li; Jian Zhang, 电子文件双套制存在的风险 ['Risks with the use of dual-copy system for electronic records management'], *Beijing Archives*, no. 3, 2009, pp. 25–26.
14. Feng, 'The co-existence of and interaction'; Tao and Tian.
15. Rong Pan, 对档案'双套制'管理的思考 ['An analysis of the dual-copy system for archives management'], *Archives World*, no. 4, 2003, pp. 20–21; Jian Peng, 关于档案'双套制'管理问题的探讨 ['Exploration of the dual-copy system for archives management']. *Archives Science Study*, no. 1, 2002, pp. 38–40; Jian Wang, 电子时代'双套制'归档的新内涵 ['An updated interpretation of the dual-copy system in the digital era'], *China Archives*, no. 12, 2004, pp. 48–49.
16. Chen; Junhua Su and Fang Liu, 被异化的谨慎 – – 对'双套制'管理的问题分析及策略选择 ['Alienated caution – An analysis of the issues with the double-copy system and copying strategies'], *Archives Science Bulletin*, no. 4, 2015, pp. 100–104; Tao and Tian; Feng, 'The co-existence of and interaction'.
17. For instance, when the second edition of the *Specification on Electronic Documents Archiving and Electronic Records Management (GB/T 18894–2016)* was issued, the dual-

copy requirement was removed. And when the revised version of *Interim Measures on the Filing and Transferring of Electronic Records (2018 Revision)* was published, it was instead required that electronic records satisfying the state's requirements could be 'filed and transferred' only in digital format (Article 7). Further, the *Outline of the 13th Five-year Plan for the Development of Archival Undertaking in China (2016–2020)* recommends pilot testing the one-track system (i.e., the exclusive use of electronic records in the conduct of business) and the one-copy system (i.e., digital records will be kept and preserved only in digital format with no extra paper or microfilm copies generated) in organisations that are suitable.

18. Yi Qian, 电子文件'单套制'管理相关概念的辨析与思考 ['An analysis of concepts related to the one-copy system of electronic records management'], *Archives Science Bulletin*, no. 4, 2017, pp. 8–13; Xinyu Shen, 电子档案'单套制'背后的电子文件管理思想转变 ['The change of the conceptual foundation accompanying the adoption of the one-copy system for digital archives'], *Archives Management*, no. 6, 2017, pp. 33–36; Xilin Shen, 电子文件单套制管理的影响因素 ['Influencing Factors of Electronic Records Management: Research Based on Expert Survey'], Master thesis, Zhejiang University, 2018; Dadong Sun and Lina Yuan, 基于SWOT分析法的电子档案'单套制'管理研究 ['Research on "Single Set" management of electronic records based on SWOT analysis'], *Archives & Construction*, no. 2, 2018, pp. 9–12.
19. For instance, in her article endorsing and advocating one-track system, Feng argues that the 'three pillars' essential for electronic records management are the legal foundation for the evidentiary capacity of electronic records, policies, and management and technologies (Feng, 'Towards Single track system') . And, in an empirical research conducted by Shen that uses an expert survey method to investigate the weight of 24 factors, which may influence the adoption of the one-copy system, the legal admissibility of digital records was given the highest weight (Shen, 'Influencing Factors of Electronic Records').
20. For instance, the *Contract Law of the People's Republic of China*, issued in 1999, recognised the effectiveness of contract in electronic form and the *Electronic Signature Law of the People's Republic of China*, issued in 2005, recognised the effectiveness of data messages in electronic form in the conduct of business activity. More recently, *Several Provisions of the State Council on Online Government Services* issued in 2019, states that 'The electronic archives that meet the archives administration requirements shall have the same legal force as paper archives' (Article 12).
21. For instance, taking the admissibility of email as an example, legal rulings show that the courts are inconsistent as to whether the authenticity of an email's screenshot can be determined without looking at the electronic version in the email client. In *Qianhai Shuliang Technology Co. LTD* versus *Beijing Hengli Jiaye Technology Co. Ltd* on disputes over advertisement contract (Case no.: (2019)-Yue-03-Min-Zhong-29168), in the first trial, *Beijing Hengli Jiaye Technology Co. Ltd* (the plaintiff) submitted a screenshot of the promotion it did for *Qianhai*'s products on VIVO promotion platform. In the second trial, *Qianhai* appealed stating that *Beijing Hengli* did not submit the original of the email in the screenshot; thus, it is incorrect for a court to determine authenticity simply based on a screenshot. In the second trial, the court stated that, 'The business between the two parties is carried out via email. In the first trial, *Shuliang* stated that its staff had resigned and therefore could not provide relevant evidence. Under such circumstance, it is not inappropriate that the court accept the evidence submitted by *Beijing Hengli*'. Yet, in *Wanwan* versus *Shanghai Yanglai Medical Equipment Co.LTD* and *Beijing Baojiali Sales Consultant Co.Ltd* on disputes over execution, the court stated, 'as for the emails, picture of *Beijing Baojiali* cash capital increase plan in 2014, and Wechat chat history submitted by *Wanwan*, because *Wanwan* did not submit the originals of the evidence, the court did not recognize the authenticity of the evidence.' These two cases show conflicting attitudes towards the form in which electronic evidence is submitted.
22. Luciana Duranti, 'The Odyssey of Records Managers', *Records Management Quarterly*, vol. 23, no. 3, 1989, pp. 3–6, 8–11.

23. Luciana Duranti, Corinne Rogers, and Anthony Sheppard, 'Electronic records and the law of evidence in Canada: The uniform electronic evidence act twelve years later', *Archivaria*, no. 70, 2010, pp. 95–124; Anthony Sheppard and Luciana Duranti, 'The Canadian legal framework for evidence and the digital economy: A disjunction?', 2010, available at <*http://ciscra.org/docs/Sheppard_Duranti_The_Canadian_Legal_Framework_FINAL_REPORT.pdf*>, accessed 10 July 2020.
24. Heather MacNeil, 'Trusting Records: the evolution of legal, historical, and diplomatic methods of assessing the trustworthiness of records from antiquity to the digital age', 1998, available at <*https://open.library.ubc.ca/cIRcle/collections/ubctheses/831/items/1.0076929*>, accessed 14 April 2020.
25. To learn more about the project, please visit <*http://www.lawofevidence.org/lede/home*>.
26. Anthony Sheppard, Luciana Duranti, Barbara Endicott-Popovsky, Corinne Rogers, Aaron Alva, and Jessica Bushey, 'Law of Evidence in the Digital Environment (LEDE) User Survey Report', 2015, p. 7, available at <*https://interparestrust.org/assets/public/dissemination/LEDE-20150128_UserSurvey_FinalReport.pdf*>, accessed 23 August 2020.
27. Donald C Force, 'Pursuing the "Usual and Ordinary Course of Business": An exploratory study of the role of recordkeeping standards in the use of records as evidence in Canada', 2013, p. 18, available at <*https://open.library.ubc.ca/cIRcle/collections/ubctheses/24/items/1.0166840*>, accessed 14 April 2020.
28. In this paper, these are identified as the three (major) procedural laws: the Criminal Procedure Law of the People's Republic of China (2018 revision) (中华人民共和国刑事诉讼法 (2018修正), the Civil Procedure Law of the People's Republic of China (2017 Revision) (中华人民共和国民事诉讼法 (2017修正)), and the Administrative Litigation Law of the People's Republic of China (2017 Revision) (中华人民共和国行政诉讼法 (2017修正).
29. See, for instance, Qifan Cui, 论民事诉讼中档案证据的运用['On the use of electronic records as evidence in civil litigations'], *Zhejiang Archives*, no. 10, 2016, pp. 14–17. Qiuhui Xiao and Binbin Duan, 我国电子文件证据地位及效力立法研究 ['A research on the legislation of evidence status and effect of electronic records in China'], *Documentation, Information & Knowledge*, no. 1, 2018, pp. 58–65.
30. See, for instance, Xuemei Cai, 电子档案凭证作用生效分析['Analysis on factors guaranteeing the evidentiary capacity of electronic records'], *China Archives*, no. 2, 2015, pp. 61–63; Kan Li, 证据法语境下电子文件的凭证性保障探析 ['On the protection of the evidentiary capacity of electronic records in the context of evidence law'], 机电兵船档案, no. 2, 2017, pp. 61–64; Xiuli Zhang, 基于电子证据认证视角的电子文件管理 ['Management of electronic records from the perspective of examination of electronic evidence'], *China Archives*, no. 8, 2010, pp. 32–34; and Xiudong Zhu and Ning Zhang, 基于证据视角的社交媒体档案管理 – 以微信为例 ['Social Media Records Management based on Evidence – Taking WeChat as an Example'], *Archives Science Study*, no. 2, 2017, pp. 63–67.
31. Xiao and Duan; Shaoxia Wang, 电子文件产生证据效力的困难及其对管理的启示 ['Difficulties encountered in the realisation of the evidentiary capacity of electronic records and their implications for electronic records management'], *Archives Science Study*, no. 3, 2003, pp. 54–58.
32. Cui; Xiao and Duan.
33. Li Xie and Guanyan Fan, 电子文件与电子证据领域中的真实性概念分析 [An analysis of the concept of authenticity in the fields of electronic records and electronic evidence], *Zhejiang Dangan*, no. 1, 2019, pp. 13–17.
34. Ran Wang, 电子文件管理与证据法规则的契合研究['Study on the alignment between electronic records management and the rules of evidence law'], *Archives Science Bulletin*, no. 5, 2018, pp. 51–56.
35. Zhiwen Huang, 电子文件的法律证据价值初探 ['A preliminary examination of the evidentiary capacity of electronic records'], *Archives Science Bulletin*, no. 2, 2000, p. 26.
36. Wang, 'Study on the alignment'.

37. A few exceptions are Lingling Ding, 电子文件法律效力的实现问题 ['On the realisation of the evidentiary capacity of electronic records'], *Yunnan Archives*, no. 2, 2011, pp. 58–59; Huang; Zhang, 'Management of electronic records'; Liang Yu and Chi Zhang, 档案证据在民事诉讼中的运用规则 ['Rules on the use of archives as evidence in civil litigations'], *Beijing Archives*, no. 3, pp. 22–23; Wang, 'Difficulties encountered in the realisation'; and Zhu and Zhang. However, instead of the best evidence rule, the authentication rule, and the exception to hearsay rule, the rules they examined are relevance, legality, and authenticity.
38. Wang, 'Study on the alignment'.
39. Nanning Zhang and Douglas Walton, 'Recent Trends in Evidence Law in China and the New Evidence Scholarship', *Law, Probability and Risk*, vol. 9, no. 2, 2010, pp. 103–129.
40. Stefan Vogenauer, 'Inquisitorial System', in Peter Cane, Joanne Conaghan and David M Walker (eds), *The New Oxford Companion to Law*, Oxford University Press, Oxford, 2008, n.p.
41. Zhang and Walton, p. 112.
42. Shujie Qi and Shengrong Zhong, 论民事审判方式改革对我国证据制度的影响 ['The Influence of Civil Adjudication Method Reform on the Evidence System in China'], *Law Review*, vol. 4, 1998, pp. 106–110, 115.
43. The Chinese original is 关于民事诉讼证据的若干规定 (2019).
44. Zhang and Walton, p. 107.
45. ibid.
46. David A Schum, *The Evidential Foundations of Probabilistic Reasoning*, John Wiley & Sons, New York, 1994, p. 93.
47. One possible explanation is that, rather than to prevent the admissibility into litigation of evidence that does not conform to the law, as claimed, the classification of evidence in the three procedural laws is a product of the investigation-centred criminal procedural mode and files-centred (i.e., case file) judgement mode. Thus, its purpose is to justify the evidentiary capacity of evidence collected and used in fact-finding in the investigation conducted by the public security bureau and presented in the case files in written form. This is why the types of evidence listed in the procedural laws reflect the steps involved in the investigation procedure specified in criminal procedural law, such as interrogation of criminal suspects, interviewing of witnesses, crime scene investigation and examination, search, and so on. See Jinsong Lin, 我国证据分类制度的功能反思 – 以刑事诉讼为中心的分析 ['Rethinking the Function of Chinese System of Evidence Classification: Focusing on the Criminal Procedure'], *Journal of Zhejiang University (Humanities and Social Sciences)*, vol. 45, no. 3, 2015, pp. 36–46.
48. It is asserted that China is one of only two countries in the world identifying types of evidence in its legislation; the other is Russia. See Lin.
49. The Civil Procedure Law of the People's Republic of China.
50. The Chinese original is 电子数据. Its English translation i.e., electronic data, was taken from the China Law Info database.
51. The Chinese original is人民法院统一证据规定(司法解释建议稿).
52. Canadian General Standards Board, Electronic Records As Documentary Evidence (CAN/CGSB-72.34–2017), 2017, p. 4, available at <*http://publications.gc.ca/collections/collection_2017/ongc-cgsb/P29-072-034-2017-eng.pdf*>, accessed 13 April 2020.
53. Much of the information regarding rules governing the admission of business records is sourced from MacNeil.
54. In this article, authenticity of records is considered inclusive of their identity and integrity, and a distinction between these two characteristics of records will only be made where necessary.
55. MacNeil.
56. The Chinese original of this term is 形式真实.
57. The Chinese original of this term is 实质真实.

58. Yingming Liu, 中美书证证据能力规则之比较 ['Comparing the Credibility of Documentary Evidence between China and the U.S.'], *Academic Exchange*, no. 2, 2012, pp. 52–56.
59. Weizhong Shi, Jing Wang and Pinger Shen, 私文书证认证规则探析 ['Exploration of the Rules for the Admissibility of Private Records'], *Journal of Law Application*, no. 7, 2010, pp. 68–71.
60. Liu, Comparing the Credibility of Documentary Evidence.
61. ibid.; Shi, Wang and Shen; Zhichao Zhao and Guilong Zhao, 民事诉讼私文书证适用规则疑难问题研究 ['On the Applicability Rules and Issues of Private Records as Documentary Evidence in Civil Litigations'], *Journal of Law Application*, no. 11, 2015, pp. 98–102.
62. The Chinese original is最高人民法院关于适用《中华人民共和国民事诉讼法》的解释.
63. The civil procedural law, Article 64.
64. Originated from the civil litigation of Anglo-American law, discovery 'is a process through which the parties to a lawsuit formally exchange evidence and information before a case goes to trial'. The most common forms of discovery include interrogatories, requests for admissions, requests for production of documents; requests for production and inspection; and depositions. See Aaron Larson, 'Conducting discovery in a civil lawsuit', 2018, available at <*https://www.expertlaw.com/library/civil-litigation/conducting-discovery-civil-lawsuit*>, accessed 22 August 2020. Discovery procedure has been called '[t]he most distinctive feature of American civil procedure', as cited in Ray Worthy Campbell and Ellen Claar Campbell, 'Clash of systems: discovery in U.S. litigation involving Chinese defendants', *Peking University Transnational Law Review*, vol. 4, no. 2, 2016, p. 134. A review of relevant literature both in Chinese and English shows that there are different understandings of the scope and substance of discovery; as a result, there are different opinions as to whether the Chinese legal system has the equivalent of the discovery process. In an earlier article published in a Chinese journal commenting on discovery in the United States, Qiao Xiongbing asserts, 'in civil law countries, there is basically no pre-trial discovery system', see Qiao Ciaobing, 也论美国的审前证据开示制度['Commenting on the American Pre-trial discovery'], *Law Review*, no. 4, 2010, p. 112. Recent research published either in Chinese or English journals shows that there is discovery in China, yet with a narrower role or different features, see Campbell and Campbell; Elizabeth Fahey and Zhirong Tao, 'The pretrial discovery process in civil cases: A comparison of evidence discovery between China and the United States', *Boston College International and Comparative Law Review*, vol. 37, no. 2, 2014, pp. 281–332. For instance, Campbell and Campbell argue that discovery does not work the same in China where litigation is judge-driven and the courts 'resolve disputes in accordance with the law and applicable governmental policies'. See Campbell and Campbell, pp. 146–147. When discussing discovery in the Chinese context, Campbell and Campbell cite clauses in the *Interpretation of the Supreme People's Court on the Application of the Civil Procedure Law of the People's Republic of China* on pre-trial evidence exchange and petition for evidence preservation, as they perceive the discovery and motion practice (specifically in the United States) as a process allowing the parties to uncover the facts and the applicable law, hence leading to a negotiated settlement payment before trial. For this understanding of discovery the clause usually cited is article 81 of *the Civil Procedure Law of the People's Republic of China (2017 Revision)* stating that, where any evidence is extinguished or hard to obtain in time, if the circumstances are urgent, an interested party may, before instituting an action or applying for arbitration, apply for evidence preservation to a people's court at the place where the evidence is located or at the place of domicile of the respondent or a people's court having jurisdiction over the case. The court performs the preservation of the evidence, and the party applying for evidence preservation shall clearly state in the motion 'the basic information of the evidence that needs to be preserved, the reasons for the motion for preservation, what preservation measures are to be adopted, and other content' (Article 25, *Some Provisions on Evidence in Civil Procedures*). In their comparison of evidence discovery between China and the United States, Fahey and Tao understand evidence discovery as a procedure involving 'one party exercising legally

regulated procedural rights to collect evidence, to discover evidence, and to investigate evidence actively and proactively' (p. 283). Stating that no Chinese law has yet clearly stipulated a discovery procedure, Fahey and Tao argue that the major aspects of evidence discovery include the following: (1) parties and lawyers conduct investigations and collect evidence; (2) the court conducts investigations and collects evidence; (3) expert evaluation; and (4) evidence exchange. They conclude that the evidence discovery system in China can be referred to as a 'discovery model led by judges' wherein the 'judge has the leading power over collection, preservation, offering, and examination of the evidence' (p. 292). Recent research published by Chinese scholars considers evidence exchange or the obligation to submit documentary evidence prior to trial as the equivalent of the discovery process. The former perspective is consistent with Campbell and Campbell's understanding. As to the latter, the obligation to submit documentary evidence is defined thus: a party or a third party who holds the evidence and yet does not bear the burden of proof has the responsibility to submit the evidence to the court, so that the court can conduct evidence investigation because the party adduces the evidence using the document as a means of evidence, as cited in Yan Zhao, 民事诉讼文书提出义务制度研究['Research on the obligation system civil procedure documents'], Master thesis, Hebei University, 2020. For this understanding of discovery, the clause usually cited is Article 112 of the *Interpretation of the Supreme People's Court on the Application of the Civil Procedure Law of the People's Republic of China* where the documentary evidence is under the control of the opposite party, the party who bears the burden of proof may submit a written application requesting the people's court to order the opposite party to submit it before the expiry of the time for adducing evidence. See e.g., Bo Gao, 电子数据偏在问题之解决 – 基于书证提出义务规则的思考 ['Resolution of the Issue of Asymmetry of Electronic Data – Based on an Examination of the Rule of the Obligation to Submit Documentary Evidence'], *Science of Law (Journal of Northwest University of Political Science and Law)*, no. 2, 2019, pp. 69–76. To summarise, there are three different understandings of discovery: discovery as a process of evidence collection and investigation; discovery as a process for evidence exchange prior to trial; and discovery as a process for a party to obtain evidence that is not under its control. In any case, discovery process in China is different from that in common law systems.

65. Jianguo Xiao, 书证的真实性及其举证责任 ['The Authenticity of Documentary Evidence and the Burden of Proof for such Authenticity'], *China Trial*, no. 53, 2010, pp. 92–93.
66. Weiqiu Long and Wei Pei, 电子证据概念与审查认定规则的构建研究 ['Concept and Authentication Rules of Digital Evidence'], *Journal of Beijing University of Aeronautics and Astronautics (Social Sciences Edition)*, vol. 29, no. 2, 2016, pp. 39–48.
67. The Chinese original is中华人民共和国合同法.
68. The Chinese original is中华人民共和国电子签名法 (2015修正).
69. The Chinese original is关于办理死刑案件审查判断证据若干问题的规定.
70. Pinxin Liu, 电子证据的收集与运用 – 以'两个证据规定'为解读 ['Collection and Use of Electronic Evidence – An Interpretation of the Two Provisions on Evidence'], *Evidence Forum*, vol. 16, no. 00, 2011, pp. 171–183.
71. The Chinese original is 关于办理刑事案件收集提取和审查判断电子数据若干问题的规.
72. The Chinese original is 公安机关办理刑事案件电子数据取证规则.
73. The Internet Court is a court of special jurisdiction in China that mainly handles Internet-related civil and administrative cases, such as disputes on online shopping contracts through e-commerce platforms, financial loan signed and performed on the Internet, ownership of the copyright of works published on the Internet, and others. Currently, three Internet courts have been established in Hangzhou, Beijing and Guangzhou.
74. MacNeil, p. 46, 50, 86.
75. Zhewei Liu, 民事电子证据: 从法条独立到实质独立 ['On the Independence of Electronic Evidence in Civil Procedure: from text to substance'], *Evidence Science*, vol. 23, no. 6, 2015, pp. 678–685.
76. Zongru Ji and Yang Niu, 论民事诉讼中电子数据的运用规则 ['Evidence Rules on Electronic Data in Civil Procedure'], *Evidence Science*, vol. 24, no. 4, 2016, pp. 448–458;

Liu, 'On the Independence of Electronic Evidence'; Chang Wang and Zhiyong Fan, 互联网金融案件中电子证据制度的适用 ['The Application of Electronic Evidence Law in Internet Finance Cases'], *Journal of Law Application*, no. 7, 2018, pp. 109–115.

77. The procedural law of civil cases, Article 64.
78. See note 64.
79. Though the Interpretations of the Application of the Civil Procedural law adopted in 2015 makes it possible for one party to request the court to order the other party to provide documentary evidence under its control (Article 112), it is not applicable to electronic data, which is a separate type of evidence. Academics in China are advocating revision of the rules for the obligation to submit electronic data evidence considering that many electronic data are very likely to be controlled by the opposing party or a third party; see for instance, B Gao, 电子数据偏在问题之解决 – 基于书证提出义务规则的思考 ['Resolution of the Issue of Asymmetry of Electronic Data – Based on an Examination of the Rule of the Obligation to Submit Documentary Evidence'], *Science of Law (Journal of Northwest University of Political Science and Law)*, no. 2, 2019, pp. 69–76.
80. For instance, in *Yaoyun* versus *Shanghai Jialong Ririzhu Information Technology Co. LTD* on disputes over service contract (Case no. (2019)-Hu-0104-Min-Chu-No. 15354), *Yaoyun* (the plaintiff) submitted his WeChat chat history with *Wang Songge*, a staff of *Jialong Ririzhu* as evidence to support his claim. *Jialong Ririzhu* admits the authenticity of the evidence, but argues that, 'because the chat history is electronic data evidence, it is possible that *Yaoyun* has deliberately concealed evidence unfavourable to him. Therefore, the chat history cannot faithfully reflect the intent of both parties.' In *Huzhou Zhulaoda Industrial Co. Ltd* versus *Shanghai Xinchisheng Trading Co. Ltd* on disputes over sales contract (Case no. (2018)-Hu-0113-Min-Chu-No.19920), the defendant (*Shanghai Xinchisheng*) submitted a screenshot of an email exchange with shopping malls and the plaintiff (*Huzhou Zhulaoda*), the plaintiff did not recognise its authenticity because the emails did not meet the requirements regarding the form of evidence, and because the source of the data could not be confirmed. The court did not recognise the authenticity of the evidence.
81. Ji and Niu; Long and Pei; Tianxin Mo, 从电子证据视角看我国证据规则的规范与完善 ['An Examination of the Refinement and Development of the Rules for the Admission of Evidence in China from the Perspective of Electronic Evidence'], *Graduate Law Review*, CUPL, vol. 31, no. 2, 2016, pp. 37–44.
82. Liu, On the Independence of Electronic Evidence; Jing Ni, 民事诉讼中电子证据的真实性认定 ['Research on Authenticity of Electronic Evidence in Civil Procedure'], *Journal of Beijing University of Aeronautics and Astronautics (Social Science Edition)*, vol. 29, no. 2, 2016, pp. 55–63; Wang and Fan.
83. This is often used when requested by the court and when the electronic data is in the form of documents, e.g., emails, instant messages, or digital photos. By printing out the electronic record, its content will be frozen; therefore, this is a way to make sure that no change can be made to the evidence in its collection, transfer, and presentation.
84. Digital evidence preservation undertaken by a notary or copyright society upon application of the parties involves collecting and freezing electronic records and providing certification of the evidence. This is the most popular approach adopted in judicial practice in the collection of electronic evidence, and the probative force of the evidence obtained in this way is relatively high. The popularity of notaries for the certification of electronic evidence and the high probative force of the evidence obtained this way is partly due to Article 9 of *Some Provisions of the Supreme People's Court on Evidence in Civil Procedures (2008 Amendment)*, which states that facts that have been proved in a valid notary document do not need to be proved by the parties concerned with additional evidence unless the submitted evidence can be overthrown by evidence to the contrary. Yet, considering the complexities inherent in verifying the reliability and authenticity of electronic evidence, the lack of reliable techniques and methods that can be used by notaries, and the lack of uniform procedural rules across districts for the preservation and certification of electronic evidence, the certification provided by the notary can at the most ensure that electronic evidence was

not altered in and after the collection process; it cannot guarantee that the evidence per se is reliable and authentic prior to collection.

85. According to the *Civil Procedure Law of the People's Republic of China*, when evidence may be destroyed or difficult to obtain at a later time, a party may, in the course of litigation, apply to the court for evidence preservation, and the court may also take preservation measures on its own initiative; the law further specifies that application for evidence preservation can also be submitted prior to litigation or arbitration. These conditions for evidence preservation are applicable to electronic evidence as well; thus, parties can apply to the court for electronic evidence preservation.
86. Ziying Lin, 论第三方电子数据平台所存储数据的证据效力['Probative Force of Data Stored in Third Party Electronic Data Platform'], *People's Judicature*, no.insert space between no. and 11, 2020, pp. 54–58. Per Article 111 of the Civil Procedure Law, when a litigation participant or any other person forges or destroys any important evidence, which obstructs the trial of the case by the people's court, the people's court may impose a fine or detention to the litigation participant or person according to the severity of the circumstances; and if suspected of any crime, the litigation participant or person shall be subject to criminal liability in accordance with the law.
87. ibid.
88. ibid.
89. Zizhu Li, 第三方电子数据平台固定电子证据的调查研究['Investigation on Fixation of Electronic Evidence by Third Party Electronic Data Platform'], 2018, n.p., available at <*https://mp.weixin.qq.com/s/Wmx-7Hbi4f3YR0wGWbv_tQ–rd*>, accessed 4 September 2020.
90. ibid.
91. Ning Cao, 电子数据第三方保全法律规制研究['Research on Legal Regulation of Third Party Preservation of Electronic Data'], 2018, Master thesis, Chongqing University of Posts and Telecommunications, p. 16.
92. 2020–2026年中国电子数据取证行业竞争格局及产业发展趋势预测报告['Current Competition Status and Development Trends Forecast Report on Chinese Electronic Data Forensics Industry (2020–2026)'], 2018, available at <*http://www.reporthb.com/report/reportview143583.htm*>, accessed 10 July 2020.
93. Zhihai Xiong and Jiabin Li, 论电子数据保全之司法应用['On Judicial Application of Digital Data Preservation'], *Chongqing Social Science*, no. 1, 2020, pp. 106–122.
94. A search of CNKI, a widely used database for academic research in China, for articles containing 'third party' and 'evidence' in its titles only returns 25 results.
95. See e.g., Min Hu, 第三方电子数据保全的应用性分析 ['The Applied Analysis of the Third Party to Preserve Electronic Data'], 2016, Master thesis, Southwest University of Political Science and Law.
96. See e.g., Cao; Feng Sun, 论电子数据第三方证据保全 ['Study on the Third Party Evidence Preservation of Electronic Data'], 2018, Master thesis, Chongqing University of Posts and Telecommunications; Li, 'Investigation on Fixation of Electronic Evidence'.
97. See e.g., Hu; Cao; and Sun.
98. See e.g., Hu.
99. <*https://www.tsa.cn/html/kxsjcfw/*>
100. Li, 'Investigation on Fixation of Electronic Evidence'.
101. Xiong and Li.
102. ibid.
103. ibid.
104. ibid.
105. ibid.
106. Li, 'Investigation on Fixation of Electronic Evidence'.
107. Xiong and Li.
108. ibid.

109. The InterPARES Trust (ITrust) (2013–2019) project – a multi-national, interdisciplinary research project aimed to develop theoretical and methodological frameworks to assist the formulation of local, national and international policies, procedures, regulations, standards, and legislation ensuring public trust grounded on evidence of good governance, a strong digital economy, and a persistent digital memory – has examined the challenges posed by the use of cloud-based services to the management of records, in particular, to the protection and demonstration of the evidentiary capacity of records, and proposed a solution to address these challenges.
110. Kenneth Thibodeau, Daryll Prescott, Richard Pearce-Moses, Adam Jansen, Katherine Timms, Giovanni Marchetti, et al., *Preservation as a Service for Trust (PaaST): Functional and Data Requirements for Digital Preservation*, 2018, p. 8, available at <*https://interpares trust.org/assets/public/dissemination/PreservationasaServiceforTrust1_0-FINAL.pdf*>, accessed 14 April 2020.
111. Luciana Duranti, 'Building a Trustworthy System: What will Trustworthy Systems Look Like in the Future?', in Philip C Bantin (ed.) *Building Trustworthy Digital Repositories: Theory and Implementation*, Rowman & Littlefield Publishing Group, Lanham, MD, 2016.
112. Thibodeau, et al., p. 89.
113. The OAIS reference model is a broad conceptual framework, developed by the Consultative Committee for Space Data Systems (CCSDS), for the preservation and access to digital information over the long term. It characterises the functional components, information objects, and environment of an OAIS-type archive, which serves as the point of reference for digital preservation requirements, and it establishes common concepts and terminologies that can encourage dialogue and collaboration.
114. Adam Jansen, 'Preservation as a Service for Trust', 2017, available at <*http://ipres2017.jp/ wp-content/uploads/5Adam-Jansen.pdf*>, accessed 11 July 2020.
115. Giovanni Michetti, 'Preservation as a Service for Trust (PaaST)', 2015 Digital Heritage, Granada, 2015, pp. 465–466.
116. Duranti, 'Building a Trustworthy System'.
117. An entity involved in executing one or more preservation capabilities. Thibodeau et al., p. 27.
118. An entity whose approval is needed for an action to be executed. Thibodeau et al.
119. An entity response for resolving a problem that occurs in preservation activities. Thibodeau et al.
120. An entity who determines if the outcome of an action is acceptable. Thibodeau et al.
121. Binary encoding is a 'specification of how an IntellectualEntity is digitally encoded and how the bit strings that contain that encoding should be processed in order to instantiate the IntellectualEntity in a form that enables it to convey information as intended'. Thibodeau et al., p. 16.
122. Adrian Cunningham, Ken Thibodeau, Hrvoje Stančić, and Gillian Oliver, 'Exploring Digital Preservation in the Cloud', in Luciana Duranti and Corinne Rogers (eds), *Trusting Records in the Cloud*, Facet Publishing, London, 2019, pp. 179–206.
123. Heuristic information is human readable information that 'supports the discovery, understanding, evaluation or use of one or more Preservation Targets'. See Thibodeau et al., p. 16.
124. Intellectual entity is an 'artefact that is intended to communicate information. Thibodeau et al.
125. Luciana Duranti, Adam Jansen, Giovanni Michetti, Courtney Mumma, Daryll Prescott, Corinne Rogers, and Kenneth Thibodeau, 'Preservation as a Service for Trust (PaaST)', in John R.Vacca (ed.) *Security in the Private Cloud*, CRC Press – an imprint of Taylor & Francis Group, Bocca Raton, FL, 2016, p. 60.
126. ibid., p. 59.
127. Cunningham et al., p. 188.
128. Li, 'Investigation on Fixation of Electronic Evidence'.
129. ibid.

Acknowledgements

The authors would like to thank the two anonymous reviewers whose comments greatly helped improve an earlier version of this paper.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This paper was based on the first author's PhD dissertation. Additional research was supported by Tianjin Municipal Education Commission Scientific Research Projects, entitled 'Rules Governing the Admissibility of Electronic Records in Civil Cases in China' (Project No. 2019SK054).

Notes on contributors

Dr. Weimei Pan is an assistant professor in the School of Management at Tianjin Normal University where she currently teaches courses on diplomatics and electronic records management. She earned her PhD from the University of British Columbia (UBC) in 2019, where she focused on the management of records as evidence and information in the context of cloud-based services in China. Her research interests include diplomatics in China, records management, archival education, and the protection and demonstration of records as legal evidence. Her current research focuses on the management of electronic records so that they can be admitted in litigations in the Chinese context and diplomatics in China.

Dr. Luciana Duranti is a Professor of archival theory, diplomatics, and the preservation of digital records in the master's and doctoral archival studies programs of the School of Information of the University of British Columbia. She is Director of the Centre for the International Study of Contemporary Records and Archives (www.ciscra.org) and of the InterPARES research project on the long-term preservation of authentic electronic records (www.interpares.org), involving, over 21 years, about 500 researchers in 42 countries. She has published extensively on the use of archival and diplomatic concepts for the understanding of new technologies, and on how to ensure the continuing trustworthiness of digital records.

ORCID

Weimei Pan http://orcid.org/0000-0003-4098-4684