FRONTIERS OF LAW IN CHINA
VOL. 7 MARCH 2012 NO. 1
DOI 10.3868/s050-001-012-0004-3

ARTICLE

TRIAL ON THE ELECTRONIC EVIDENCE: CHINA'S RULES ON ELECTRONIC EVIDENCE

Pinxin Liu[*]

How to use electronic evidence to decide cases has become a major conundrum in Chinese judicial practice. Starting with an analysis of a typical case, this article discusses two basic ideas of electronic evidence in deciding cases, points out the distinctions between scientific proof and judicial proof, and concludes that it should follow the road of judicial proof by suitably referring to the principle of scientific proof. On the basis of such discussion, it further expounds on the models and the mechanisms of electronic evidence. In addition, considering Chinese traditional theory of evidential law and learning from the proving method in historiography, it puts forward the theory of evidential system for electronic evidence in the virtual space. Finally, it focuses on how to deal with the digital alibi in practice and arrives at a solution by managing those theories comprehensively.

INTRODUCTION ····· 75
I. BASIC VIEW OF ELECTRONIC EVIDENCE TO DECIDE CASES: SCIENTIFIC PROOF OR JUDICIAL PROOF? ····· 77
II. BASIC MODEL OF ELECTRONIC EVIDENCE TO DECIDE CASES: REGULATED PROOF OR FREE PROOF? ····· 79
III. BASIC MECHANISM OF ELECTRONIC EVIDENCE TO DECIDE CASES IN CHINA: BY SINGLE EVIDENCE OR JOINT EVIDENCE? ····· 83
IV. CONSTRUCTING CHINA'S ELECTRONIC EVIDENCE RULES ····· 85
V. SOLUTION OF DIGITAL ALIBI ····· 88
CONCLUSION ····· 89

[*] Ph.D and Associate Professor in law, School of Law, Renmin University of China, Beijing, China. Special thanks to professors Zongzhi Long, Bin Zhang, and Shijian Dai for their illuminating points on this article. This research is funded by the Project of Key Laboratory of Evidence Science by China University of Political Science and Law and the Ministry of Education in China (no. 2010KFKT07). Contact: liupinxin@gmail.com

INTRODUCTION

As brand-new evidence with high technology, electronic evidence has been playing an increasingly important role in solving legal disputes. In the meantime, it has also brought all kinds of impacts and challenges into the legal system regarding evidence in each country, such as how to collect and keep electronic evidence, how to review and admit electronic evidence, and especially, how to effectively decide cases based on electronic evidence. The final issue has been becoming a formidable challenge in practice. Now I take a common case with extensive arguments as an example.

> 【Case 1】 One day, a public security bureau in China received a call from Lin who said that his ID and password of e-mail had been stolen by someone who had used his account to send an e-mail attaching seven pornographic photos to his colleague Li, which had incurred very bad effect. The Public Security Bureau examined the e-mail and the logs of the Municipal Telecommunication Office's server and discovered that the IP address of the computer from which to send the sexual e-mail was "61.146.82.94"; from the consumers' list of accessing Internet in the Municipal Telecommunication Office, at the time when this case happened, the telephone number of that IP address was "341xxxx," and the account number of Internet access was "e 183 test," which belonged to Liang. In addition, the Public Security Bureau also found that the name of the machine that was recorded by Li's computer when receiving the e-mail through the Municipal Telecommunication Office's server was the same as the name of Liang's computer. When sending the sexual e-mail, Liang was accessing the Internet alone at home, so he had time to commit the offence. Therefore, the Public Security Bureau interrogated Liang and seized his computer. Liang received an administrative warning punishment and a fine of 1500 RMB. Liang did not accept the decision and lodged an appeal to overrule the administrative punishment with the reason that it might be some hacker who had stolen his e-mail account and had committed the offence.[1]

It was regarded as the first case in which the IP address was used as evidence in China. During the trial, the key argument was whether the plaintiff was successfully proved to have committed the illegal behavior of sending

[1] Jun Zheng, Nanjian Zhao & Qingchun Zeng et al, IP 地址首次作证网民败诉 (The Netizen Lost Lawsuit in Taking IP Address as Witness), 南方日报 (Southern Daily), May 27, 2003.

pornographic photos by the evidence collected, which included not only the electronic evidence such as IP address, e-mail, and logs, but also the traditional evidence such as the party statements and witness testimony. The key point is how to combine these two kinds of evidence to decide the case. Obviously, what kind of judgment would be reached by the court will mainly depend on how to use these electronic evidences.

This is a legal problem that is related to, and also differs from the evaluation of the probative force of electronic evidence. In brief, the evaluation of the probative force of electronic evidence is usually the basis of electronic evidence to decide a case; the latter is an extension of the former. The general principles of these two are identical. Therefore, the mechanisms of dealing with these two problems are the same in Western countries; in other words, the traditional principle of discretion still governs.

However, there is no typical principle of discretion in China. Can the judicial experience from foreign countries be simply used by China? Up to now, the theoretical society has paid little attention to this problem and the practical society is often in difficulties resolving relevant issues. It is very often that in the cases of murder or theft, although the accused's evidence seems rather strong in court, the defense puts forward some electronic evidences such as e-chatting records to prove that the defendant had no time to commit the crime, which is called a digital *alibi*[2] in Western countries. How to deal with such kinds of electronic evidence will be evidential obstacles faced by criminal judges. In some cases, judicial personnel made great efforts to decide cases; but still, the judgments are easily questioned by different people and even lead to disputes between the scientific and legal societies.

How to solve such a complicated evidential problem has been an emergent task for the judicial society in China recently. Starting with the tradition of judicial proof in China, this article discusses the idea, model, and mechanism of electronic evidence to decide cases, and then puts forward the electronic evidence rules to decide cases under national conditions. Considering that there are some similarities between the proving method of historiography and that of judicial proof, this article also compares with, and learns from, some theories of the proof of historiography.

---

[2] Eoghan Casey, *Digital Evidence and Computer Crime*, Academic Press (London), at 199 (2000). "*Alibi*" means that evidence proves that a person was in another place at the time when a crime happened. This is a very common defense for innocence in the criminal procedure. The digital *alibi* refers to electronic documents, such as the records of Internet chatting, e-mails, or the records of browsing the Internet, etc.

I. BASIC VIEW OF ELECTRONIC EVIDENCE TO DECIDE CASES: SCIENTIFIC PROOF OR JUDICIAL PROOF?

Electronic evidence is the product of information technology, while its application is mainly in the judicial society. On the surface, judges should obey all kinds of principles and rules of judicial proof when using electronic evidence to decide cases. However, electronic evidence is usually collected and evaluated by technical experts. The expert opinion (or expert conclusion) plays an important role in proving the facts of a case. So the first question for judges is whether to rely on the judicial proof or the scientific proof as instruction when they use electronic evidence to decide cases.

In the above case, after discussion of the judicial committee, the court of first instance held: The receiver of the sexual e-mail displayed that this e-mail came from Liang's computer, and the IP address, the Internet telephone number and account number all belonged to Liang. In addition, the consumers' list of Internet access from the Municipal Telecommunication Office also displayed that Liang was accessing Internet at his home alone through telephone, and Liang admitted it; the Public Security Bureau found that Liang's computer was not attacked by a hacker after examining his computer, and concluded that it was impossible for a hacker to commit the offence. Therefore, the IP address, Internet account number and e-mail password, which are of unity and exclusivity, are enough to prove that the sexual e-mail were sent from the computer which was being used by Liang at that time.[3] The judgment was made by the court of first instance mainly relying on the legal reasoning and judicial discretion, which obviously belongs to the typical idea of judicial proof.

This judgment was decided by the judicial committee members collectively, which was very prudent, and it was upheld by the Intermediate Court and supported by the legal society. However, it was questioned extensively by many technical experts. In 2005, Zeming Yang, who is from the Institute of High Energy Physics at Chinese Academy of Sciences, interpreted this case during an academic conference. His criticism was that there was insufficient evidence to prove that the plaintiff had committed this illegal activity. It was not scientific to decide the Internet behavior only by the IP address. The court should collect more evidence by gaining online evidence, recovering HDD data, and analyzing disk-fragments.[4] In 2006, I also addressed a speech analyzing this case at the

[3] See Zheng, Zhao & Zeng et al, fn. 1.

[4] See Zeming Yang, 计算机取证与日志分析 (Collecting Evidence from the Computer and Analyzing Logs), the Annual of Emergency for the Safety of Computer and Internet as well as the Annual Materials of the Work Committee for the Safety of Computer Internet and Information under the Internet Association of China in 2005.

2nd Annual China Computer Forensics Conference (CCFC), but most other computer experts attending the academic conference put forward different opinions. Someone even said that if the court could decide the case under such circumstances, then any computer expert might control other people's computers as a hacker to commit illegal activities in the name of others. Compared with these two technological experts' opinions, it is obvious how different the views of technological experts and legal experts are on electronic evidence to decide cases.

In fact, it is somewhat fashionable for technological experts to disagree with the judicial judgments in contemporary society. These disputes are the results of different ideas between the scientific proof and the judicial one.

First, the scientific proof takes natural phenomena as objects, which is not restricted by the proving means, but the judicial proof takes social disputes as objects, which requires that the proving process should abide by the spirit of rule of law and should not permit all parties to prove something at will.

Second, the scientific proof usually has no requirement for time limit, but the judicial proof should be finished within the statutory time. The whole process of collecting judicial proof is stressful and requires high control capability, which is called "a prescription of judicial proof." Collingwood has already evaluated such characteristics of the judicial proof and said: "If any juror says: 'I think it may confirm, after a year, when we can recall that kind of evidence freely, we will be in a better position to see what it will mean.' Then the answer will be: 'What you say sounds reasonable, but it is impossible to realize your proposal. Your obligation is not only to judge a case, but also to judge it now. So you have to stay here till you make your judgment.' "[5]

Third, the scientific proof is done by an expert in a specific area, but the judicial proof is generally done by a judge who is a layman and lacks knowledge of the technology.[6] Therefore, the process of scientific proof is controllable, repeatable, and verifiable, while the judicial proof has difficulty in obtaining an effective external validation.[7] This is basic difference between the two methods.

Today, as people increasingly respect science, the scientific proof has brought deep influence on the judicial proof. Nevertheless, the judicial personnel are not scientists, and the judicial proof is not the scientific proof, of which the purpose is to find the truth at most, either. In the scientists' view, the judicial proof (the

[5] R. G. Collingwood, *The Historical Idea*, translated into Chinese by Zhaowu He and Wenjie Zhang, The Commercial Press (Beijing), at 371 (1997).

[6] See Haoran Chen, 证据学原理 (Principles of Evidence Science), Huadong Science and Technology University Press (Shanghai), at 25 (2002).

[7] See Zongzhi Long, "大证据学" 的建构及其原理 (The Structure of "Science of General Evidence" and Relative Theories), (5) 法学研究 (Chinese Journal of Law) 82, 95 (2006).

crystal of human's common judicial experience) looks like a very strange set of a man-made device. However, the judicial proof has a long history and will exist forever. The scientific proof cannot completely take the place of it.

From this point, to solve the problem of electronic evidence to decide cases, we cannot wholly follow the scientists' idea. On the one hand, the purpose of using electronic evidence is not only to discover the truth, but also to settle disputes, therefore it is necessary to follow the legal system regarding evidence as the way of treating traditional evidence. On the other hand, the forensic computer science is at the preliminary stage in the world; it is very difficult to reach an agreement by experts in different fields on the effectiveness of electronic evidence. Therefore, it still belongs to the category of judicial proof in nature, and it may receive a favored judgment when the evidence meets the standard of proof.

Actually, such kind of judicial proof needs the help of electronic evidence that is discovered by high technology, and it may refer to some principles of scientific proof. That is to say, when a judge gives judgment, he should follow the information revealed by judicial proof and take into account of the characteristics of technology and expert opinions.

II. BASIC MODEL OF ELECTRONIC EVIDENCE TO DECIDE CASES: REGULATED PROOF OR FREE PROOF?

Though the judicial proof is very complicated in society, it has two basic models: regulated proof and free proof.[8] The former refers to that the law stipulates detailed rules for the activities regarding judicial proof, and that judicial personnel should abide by these rules when applying evidence to ascertain a case's facts; the latter refers to that there is no limitation stipulated by the statutes for the activities regarding judicial proof, so the judicial personnel can freely apply evidence to ascertain a case's facts. The fundamental distinction between them is whether the judges or jurors have freedom to use evidence to find the facts of a case.

In the Middle Ages, the system of evidence in Roman Law belonged to a typical model of regulated proof in Roman Law. At that time, a fundamental principle was followed — "If there is a *plena probatio*, it should give a favored judgment; if there is no *plena probatio*, it should not give a favored judgment." So, what is a *plena probatio*? The system assigned "a predetermined value to every evidentiary element" and used "a complex of arithmetical rules .... Thus

[8] See Jiahong He, 从司法证明模式的历史沿革看中国证据制度改革的方向 (Trends of Reforming Chinese Evidence System — from the Historical Evolution of Judicial Proof Modes), (4) 法学家 (Jurist) 123, 123 (2005).

one unexceptionable witness constitutes half proof (*semi-plena probati*), but one doubtful witness (*testis suspectus*) makes less than half proof (*probatio semiplena minor*), while one unexceptionable witness plus one doubtful witness makes more than half proof (*probatio semiplena major*). Common repute (*fama*) comparison of writings (*comparatio literarum*) and private documents (*privata scriptura*) are reckoned as other species of half proofs."[9]

At the end of 18th century, countries in Europe replaced the regulated proof model with the system of "free evaluation of evidence through inner conviction," which is a typical model of free proof. For example, since 1808, French Criminal Procedure Code has a special provision, as follows:

> The law does not ask the judges to account for the means by which they convinced themselves; it does not charge them with any rule from which they shall specifically derive the fullness and adequacy of evidence. It requires to question themselves in silence and reflection and to seek in the sincerity of their conscience what impression has been made on their reason by the evidence brought against the accused and the arguments of his defense. The law asks them but this single question, which encloses the full scope of their duties: Are you inwardly convinced?[10]

That is to say, the judge or the juror has to freely judge a case by applying "all human common perceptibility." Actually, such kind of free proof has been changing from an absolute free proof to a relative free proof as time has passed. When deciding a case, a judge has to accept the outer restrictions, such as the rules of experiences, rules of logic, and openness of free evaluation. Comparatively speaking, there was no such similar change of models in the common law legal system. It totally belongs to the model of free proof, and the judge or the jury enjoys great discretion in deciding a case by reviewing evidence.

Therefore, as to using electronic evidence to decide cases, what kind of model should be chosen? The answer does not only depend on the present system of evidence law in each country, but also involves the characteristics of electronic evidence. As the model of free proof is commonly used in two legal systems, it seems that the electronic evidence should be evaluated freely with the discretion of the judge or juror. However, to some extent, the effect of the model of free proof is closely related with the decider's quality, especially the professional experience. The reality is that the judge or juror is not familiar with information technology. Due to his/her lack of basic information knowledge, there is no doubt

---

[9] See Edmund M. Morgan, *Hearsay Dangers and the Application of the Hearsay Concept*, 62 Harv. L. Rev. 177, 181 (1948).

[10] See Julius Stone, *Evidence: Its History and Policies*, W. A. N. Wells (ed.), Butterworths (Sydney), at 16 (1991); Legifrance, *Code of Criminal Procedure* (2003), art. 353, at http://www.legifrance.gouv.fr/html/codes_traduits_cpptextA.htm (last visited Apr. 8, 2011).

that it lacks the basic legitimacy and feasibility for the judge or juror to decide cases by electronic evidence.

On the contrary, what will happen if people choose the model of regulated proof? An assumption of "Utopia" is that the legislator issues a detailed list of probative force for electronic evidence in advance, and during the process of trial, the judge or the juror will use the electronic evidence accordingly. However, up to now, no one has been able to make "such table" and it is impossible to do it in the future as well. Since when deciding a case by the way of combining electronic evidence with other evidence, it essentially requires the judicial personnel's subjective action to make this evidence a full force. So it is a daydream to completely rely on legislative stipulations.

This conclusion has been proved by the development and the change of the relevant systems of evidence during the period from the recent 30 years in the world. Early in 1992, the United Nations Commission on International Trade Law pointed out in the report of the Legal Issues of Electronic Data Interchange that in some countries, the probative force of electronic evidence is judged by the court considering several factors, such as the safety of the computer's system, whether the computer has worked correctly, as well as other factors affecting the reliability of electronic evidence; in other countries, it depends completely on the court's discretion to decide cases.[11] In other words, the basic models used by foreign judges in evaluating the probative force of electronic evidence are either the complete free proof, or the relative free proof, which are also two models of the use of electronic evidence to decide cases applied by foreign judges. Such tradition has come down without any essential change until now.

The mechanism of the relative free proof here refers to international organizations or states stipulating some referential standards to instruct the judge or juror on how to decide cases based on electronic evidence. For example, Section 4(2) of the Computer Evidence Act 57 (1983) in South Africa stipulated that "in order to assess the evidential weight of an authenticated computer print-out, the court may (a) take account of anything contained in the authenticating affidavit or a supplementary affidavit; (b) on the application of any party to the proceedings require the deponent to the authenticating affidavit or a supplementary affidavit or any other person to testify orally on any topic relevant to such question, whether or not any such affidavit covered it."[12] This is a method of assessing the weight of electronic evidence by any authenticating affidavit, supplementary affidavit or oral testimony. For another example, article

[11] United Nations Commission on International Trade Law, *Legal Issues of Electronic Data Interchange*, paras. 44–45, at http://www.uncitral.org/pdf/english/yearbooks/yb-1991-e/vol22-p381-397-e.pdf (last visited Apr. 7, 2010).

[12] Sect. 4(2), Computer Evidence Act 57 of South Africa of 1983.

9(2) of the UNCITRAL Model Law on Electronic Commerce (1996) stipulated that "information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor."[13] This article establishes a non-discrimination principle on the assessment of the evidential weight of data messages and provides some useful guidance as to how the evidential value of data messages should be assessed (e.g., depending on whether they were generated, stored or communicated in a reliable manner).[14] Besides, rule 7 of the Rules on Electronic Evidence in Philippines also provides six referential factors in assessing the evidentiary weight of an electronic document.[15]

The above stipulations are common experience of judicature. Actually, they are only related to the evaluation of the probative force of electronic evidence, and have no direct useful value from the perspective of deciding cases by using electronic evidence. Even regarding the evaluation of the probative force of electronic evidence, there is also a question concerning the practical significance of the above reference standards. For example, the Computer Evidence Act of South Africa (1983) was abolished in 2002.[16] As to the UNCITRAL Model Law on Electronic Commerce, although it is a model law for promoting the legislation of electronic business, the Canadian Uniform Law Committee formulated the Uniform Electronic Evidence in 1998 by referring to it, but finally did not adopt similar provisions because there was too much controversy in article 9(2) of the Model Law on Electronic Commerce.[17]

The academic society in China has made helpful exploration in this aspect. Prof. Jiahong He and I edited a book — *Study on Law of Electronic Evidence*, which tried to put forward three rules on how to evaluate the probative force of electronic evidence: (a) The probative force of the notarized electronic evidence is stronger than the one which is not executed by a notary public; (b) the electronic evidence produced during the routine business is of stronger probative force than that produced for the purpose of lawsuit; (c) the probative force of electronic evidence that holds against himself is strongest, the one that the

---

[13] Art. 9(2) of UNCITRAL Model Law on Electronic Commerce.

[14] United Nations Commission on International Trade Law, *Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce*, para. 71, at http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf (last visited Apr. 7, 2010).

[15] Rules on Electronic Evidence of Philippines, rule 7, sect. 1.

[16] Electronic Communications and Transactions Act of South Africa (2002), sect. 92.

[17] Amelia H. Boss, *The Uniform Electronic Transactions Act in a Global Environment*, 37 Idaho L. Rev. 275, 321 (2001).

neutral party holds is middle, and the one that holds beneficial to himself is the weakest.[18]

This view has been expanded by many young scholars throughout many years. For example, Xin Lü supplemented three more rules: (a) The electronic evidence made by expert opinions has much stronger probative force; (b) the reviewed electronic evidence has much stronger probative force; (c) the electronic evidence by a qualified attested organization's certificate has much stronger probative force.[19] Ye Li added another rule that "the probative force of the electronic evidence provided by the attested organization is stronger than that collected by the party himself."[20] In the same way, these rules are valuable in evaluating the probative force of electronic evidence. However, it does not tell the judicial personnel how to decide cases by electronic evidence.

To sum up, we can see that neither the simple model of regulated proof nor the simple model of free proof can solve the problem about how to use electronic evidence to decide cases. We should combine the two models when deciding cases based on electronic evidence and summarize the standards and rules in each country regarding the use of electronic evidence to decide cases on the basis of the tradition of judicial proof. These standards and rules, including the standards of all kinds of electronic technology or information technology issued by various organs or trade organizations, should be enacted mainly in the form of legislature to guide the practice.

III. BASIC MECHANISM OF ELECTRONIC EVIDENCE TO DECIDE CASES IN CHINA: BY SINGLE EVIDENCE OR JOINT EVIDENCE?

After determining the basic model of electronic evidence to decide cases, the next step is to examine its mechanism, which is mainly concerned with the question about whether a case can be decided by single evidence. It is another issue in close relationship with a traditional theoretical dispute in China, no matter how the electronic evidence is direct evidence or indirect evidence. One viewpoint holds that "the electronic evidence is easily counterfeited or juggled, and there is no trace left after being counterfeited or juggled. So it is indirect evidence, which cannot prove a case's facts directly and solely."[21] However,

[18] Jiahong He (ed.), 电子证据法研究 (Study on Law of Electronic Evidence), Law Press (Beijing), at 158 (2002).

[19] Xin Lü, 民事诉讼中电子证据研究 (Study on Electronic Evidence in Civil Procedure), Thesis of Master's Degree at China University of Politics and Law, at 46 (2006).

[20] Ye Li, 电子证据证明力研究 (Study on the Probative Force of Electronic Evidence), Thesis of Mater's Degree at Jinan University, at 32 (2007).

[21] Xuemei Bai & Zhanli Sun, 电子证据中的法律问题 (Legal Issues of Electronic Evidence), 计算机世界 (China ComputerWorld), Sept. 7, 1998.

many scholars do not agree with such views.

In fact, the standard of division between direct evidence and indirect one is the relationship between the relative evidence and the main facts of a case. In order to judge whether the electronic evidence belongs to the direct evidence or indirect one, we should consider whether the electronic evidence can solely prove a fact in issue, or if it needs other evidence to prove it. In China, the scope of electronic evidence is very extensive, including electronic material evidence, electronic documentary evidence, electronic audio-visual materials, electronic witness testimony, electronic statements of parties, expert conclusions of electronic evidence, as well as electronic records of inquests and examination.[22] All these kinds of forms of electronic evidence can be direct evidence or indirect evidence, depending upon the actual conditions. For example, in a case involving invading computers where the criminal left some electronic traces in the system of the invaded computer, these traces usually belong to indirect evidence; but in a case of electronic business where two parties signed a business contract by e-mail, such e-mail might be direct evidence. Anyway, whether electronic evidence is direct or indirect is a natural attribution, it will not change with the outer system, such as stipulations of law. So assigning the whole electronic evidence to the indirect evidence is obviously one-sided.

It is also wrong that only indirect evidence is not sufficient to prove the facts of a case without other supplementary evidence. It is necessary to verify direct evidence with other evidence in order to prove the facts in question. The mainstream of procedural theory in China is instructed by the dialectical materialism that stresses the verified relationship between each other to ensure that the evidence is true and sufficient. The truth of single evidence cannot be affirmed by itself, even if the content itself and the provider's character are beyond question.[23] For example, a piece of documentary evidence can directly prove the relationship of the parties by its contents, but its authenticity needs to be proved by other evidences.

Underlying such a phenomenon is the general principle that "single evidence is not sufficient to prove the facts of a case." It seems from the rule that "single evidence cannot be cited" in the historical science of China. Here "citation" means proving his own view by citing words from historical materials, ancient books and records. It is a taboo to make a point based on single evidence. As what Qichao Liang said, a single evidence cannot support a fixed view. If there is no counterevidence, a fixed view is reached; if there is continuing evidence, it is

[22] Pinxin Liu, 中国电子证据立法研究 (Study on Creating Chinese Electronic Evidence Rules), China Renmin University Press (Beijing), at 187–91 (2005).

[23] Jianming Li, 刑事证据相互印证的合理性和合理限度 (Rationality and Reasonable Limitation of Verified Criminal Evidence), (6) 法学研究 (Chinese Journal of Law) 20, 23 (2005).

to believed gradually; if there is strong counterevidence, the conclusion reached from the single evidence should be given up.[24] The principle of "a single evidence cannot support a fixed view" in historiography is introduced into the procedural law, and becomes "single evidence cannot decide a case." It is explained that "a single evidence cannot decide a case" refers to "the evidence itself cannot prove the existence and the degree of its probative force. We have to combine all evidences and consider all conditions to decide the probative force of evidence reasonably, including the circumstances of the evidence, the contradiction between this evidence and other evidences, the verification by each other, and the position of the evidence in the whole system of evidence of a case."[25]

When applying such mechanism to use electronic evidence to decide cases, it means that the electronic evidence cannot stand alone to prove relevant facts. There is no "single electronic evidence that is sufficient to verify a case." We should always combine the electronic evidence with some auxiliary information and other evidence to acquire comprehensive verified evidence to determine facts and to decide a case. In a word, no matter whether it is direct evidence or indirect evidence, any electronic evidence does not play the role solely but functions together with other evidence within the system of evidence to prove the facts of a case.

IV. CONSTRUCTING CHINA'S ELECTRONIC EVIDENCE RULES

The system of evidence is not a new concept in China. It refers to a whole system in which some interdependent and related evidence are combined. Among them, the evidence used to decide a case must be one linked with another and called as a chain of evidence. The system to decide a case should meet the requirements not only in quality, but also in quantity, and the key point is that the evidence used to prove the main facts of a case should be verified. From this point of view, the system is related with the verified proof. Some scholars called the system of evidence law in China as the "model of verified proof," namely, one piece of evidence must be verified by another evidence, and all evidences used to determine the facts of a case must be verified."[26]

---

[24] Qichao Liang, 清代学术概论 (Academic Conspectus on Qing Dynasty), Shanghai Press of Ancient Books and Records (Shanghai), at 47 (1998).

[25] Ruihua Chen, 理想与现实——从实证的角度看中国的刑事审判方式改革 (Ideal and Reality — on the Criminal Trial's Reform from a Practical View), cited from: Peking University Law School (ed.), 刑事法制的理念建构 (Ideal Construction of Criminal Legal System), Law Press (Beijing), at 416 (2002).

[26] See Li, fn. 23 at 20.

"The model of verified proof" belongs to "the model of free proof," but is very different from "the typical model of free evaluation of evidence through inner conviction" in the Roman legal system. It pays more attention to the evidence's "externality," instead of the evidence's "introversion." Namely, single evidence is not enough to prove something and it must gain support from other evidence containing similar information, which is an "objective verification," so does the electronic evidence. This is the natural meaning of deciding cases based on a system of electronic evidence.

Compared with the system of traditional evidence, the system of electronic evidence has its own characteristics. They can be divided into two categories: (a) the evidence system in physical space, and (b) the one in virtual space. The former refers to some electronic evidence verified with traditional evidence and jointly forming a chain of evidence between the virtual and the physical space; the latter refers to some electronic evidence verified with each other and forming a chain of evidence in the virtual space. This function of proof for the two categories is not the same.

In the above case, the court of first instance stated the facts that the plaintiff committed illegal activities of sending sexual e-mails could be further divided into two aspects: One is that the sexual e-mail in the above case was sent by the plaintiff's computer at some time; the other is that at that time when committing illegal activities, the plaintiff was using his computer alone at home.[27] The first fact only involved the virtual space, of which the principal evidence was electronic evidence, such as e-mail, IP address, the Internet account number and password, etc. The second fact of the case involved the evidence mainly like the Internet list by the Municipal Telecommunication Office against the specific IP address and the plaintiff's statement. Whether these two strings of evidence can form an independent system of evidence, in other words, whether all kinds of evidence can be verified with each other within the two independent systems, is the basis for the judge to make a definite verdict.

Comparatively speaking, the first system of evidence seems distinctive and important. It refers to a virtual space and relies on various kinds of electronic evidence. The traditional evidence can play a little role. Therefore, it seems much more important to hold the compositions of electronic evidence correctly.

From the perspective of composition, the electronic evidence may be divided into data message and auxiliary information evidence. The former refers to the data text itself, which records the data of occurrence, change and loss of the legal relationship, such as e-mail, EDI text; the latter refers to the records about the

[27] As for the fact that whether there was a hacker infringing the plaintiff's computer during that time, it constitutes a minor fact. After the defendant, the public security bureau, provided basic evidence, the burden of proof should be shifted to the plaintiff, Liang.

production, storage, transferring, amendment, additions and deletions, such as the logs of the electronic system, the attributive information of electronic documents, etc. They play different roles of proof. The former is mainly used to prove the legal relationship or relevant facts; the latter is mainly used to prove that the data message is real and reliable, including that by which computer's system the data message is produced; at what time it is produced; by which computer's system and on which medium it is stored; by which computer's system or IP address the e-mail is sent; and by which password and which computer's system the data message was amended, added or deleted, etc. The latter should constitute a complete chain of evidence just like the traditional evidence, so as to protect the electronic evidence perfectly in each stage, which means that the electronic data can be reviewed in each stage by other evidence from the formation to the collection, or even until being offered in the court; and that all evidences can form a custodian chain of evidence, too.

Accordingly, to evaluate whether the court made a proper judgment or not, we should not simply apply the standard used by the technological experts, but should consider it within the specific legal system regarding evidence. In China, we have to examine whether all evidences of the case constitute a complete system of evidence. In the above case, the main data message was the sexual e-mail collected from the receiver and the auxiliary information evidence was other information such as the IP address, Internet telephone number and account, etc. If the Public Security Bureau could collect another e-mail from the sender and the Internet server — the Telecommunication Office or the electronic e-mail station, of the same content as the one collected from the receiver, and in the meantime check the auxiliary information, such as IP address, sending time, sending route, etc. (verified with each other and no unusual information), then such a system of evidence would be more solid and would reduce the possibility of making mistakes.

To explain further, the verified standard may refer to "dual evidence methods" which prevails in the historical society in China created by the historian, Guowei Wang. In 1925, Wang stated in his book — *New Evidence for Ancient History* that: "We were all living in such an age. It is very lucky to have not only paper records but also new materials underground. By such material, we may supplement paper records and can prove that part of the ancient book is a real record, that is to say, paper records may only reflect one side of the facts. Such dual evidence methods can only be done today. Although it cannot be denied that some part of the ancient book has not been proved yet, it is certain that what had been proved have been affirmed."[28] That is to say, the historical

[28] Guowei Wang, 古史新证——王国维最后的讲义 (New Evidence for Ancient History — Final Teaching Materials of Guowei Wang), Tsinghua University Press (Beijing), at 2–3 (1994).

study has to combine "paper records" with "underground materials" and they are verified with each other. Why to do it in this way? The essence is to require that only when materials from different independent origins point to the same object can the historical judgment be made. Of course, it will not exclude the triplicate evidence methods, even the multiple ones.

As to archeology, "paper records" and "underground materials" are evidences from different independent origins; as to the judicial electronic evidence, the data message coming from different computers are of different independent origins (because they are the products of different computers' operation). If they are unanimous, it means that the auxiliary information evidence is verified and the judicial personnel can decide a case. This is the system of evidence in the virtual space. As to why the court may decide a case when the electronic evidence from the virtual space can be verified by the traditional evidence from the physical aspect, it is also because they have different independent origins. In conclusion, only when the origin is independent, can the case be decided based on the electronic evidence from those origins.

V. SOLUTION OF DIGITAL ALIBI

Traditionally, *alibi* is an important defense. If in the court, the defendant said that he was sending e-mails, browsing news or buying something online, this might form a digital *alibi*. It can support the defense provided by the defendant that he has no time to commit the crime and the facts of the case can be made clear by examining and evaluating the digital *alibi*.

【Case 2】 A and B are sister and brother. They were prosecuted for having entered into an electronic storehouse, having killed the housekeeper, and having stolen the valuable electronic products at two o'clock in the morning on June 13, 2004. In the beginning, the prosecution's evidence was rather strong; however, in the court, the two defendants suddenly began to overturn their statements. B denied that he committed the killing and stealing, and A also said that her brother B did not go to the scene of crime. The defense lawyer also offered an MSN record to prove that from 8:00 p.m. in the night before the occurrence of the crime to 5:30 a.m. the next morning, B was in the Internet bar for e-chatting. The lawyer also provided the records of Internet chatting during that period to the court. Then the judicial personnel were puzzled about how to review the evidence of Internet record, which was intended to prove that B had no time to commit the crime.

In this case, the defense lawyer put forward an affirmative pleading that the defendant had no time to commit the crime, and the relative evidence was mainly

the record of Internet chatting — a digital *alibi*. Then, can the judicial personnel accept the *alibi* defense relying on such electronic evidence?

American Scholar, Eoghan Casey pointed out that "investigators should not rely on one piece of digital evidence when examining an *alibi* — they should look for an associated cybertrail."[29] These traces include not only the statements of those people who are familiar with computers and the Internet, but also the electronic documents, logs of computers, and Internet information. From the perspective of technology, the electronic evidence itself cannot prove where someone stayed at some specific time. The IP address is related to a computer, not somebody. Therefore, an accessory may counterfeit the *alibi* evidence by using the principal criminal's computer. The time information may be modified in some computers in order to pretend that the criminal is not at the crime scene. However, the investigator can find the counterfeiting traces by checking the computer's trails. Eoghan Casey supports that with a case below:

> 【Case 3】 On 19 March 1999, an individual broke into the Museum of Fine Arts in Boston and stole a precious object. Security cameras show a masked burglar entering the museum at 8:00 p.m. and leaving at 8:30. The prime suspect claims to have been at home in New York, hundreds of miles away from Boston, when the crime was committed. According to the suspect, the only noteworthy thing he did that evening was to send an e-mail to a friend.[30]

Regarding this so-called e-mail, investigators may verify its credibility by checking its message header and log entries from the mail servers.

In my opinion, facing a digital *alibi*, we have to look for other evidence to confirm that the defendant has no time to commit the crime. In case 2, the judicial personnel faced a difficult problem of whether the court could confirm that the defendant had no time to commit the crime only based on a record of Internet chatting. If the judicial personnel could find more than two records of Internet chatting or e-mails originated from different computers and of coherent contents of data text, and the auxiliary information is consistent, then the case could be decided. If only one record of Internet chatting or e-mails could be found, it is necessary to see whether it is consistent with other traditional evidence. In a word, a system of evidence is quite necessary in deciding a case.

CONCLUSION

At present, it is striding into the society of information. Some predict that the

[29] See Casey, fn. 2.
[30] Id. at 202–03.

electronic evidence will become the new king of evidence. To ensure the scientific use of electronic evidence to prove the facts of cases, the key point is to make a strong system of evidence for the virtual space with all efforts. It has been becoming an issue of the era for the law of evidence.

Based upon the reality of China, and learning from foreign countries about the application experience of the rules of electronic evidence, especially by referring to the theory of historical proof of "dual evidence methods," this article tries to analyze the idea, the model, the mechanism, and the rules of the use of electronic evidence to certify cases, and puts forward the theory of evidential system for electronic evidence creatively. Among these, the theory of evidential system of the virtual space is worthy of earnest attention and reference by the legal and the practical societies in China. In addition, from a developmental viewpoint, this theory should be transformed into China's reinforced rules of electronic evidence soon.