E-Business Law in China: Strengths and Weaknesses

AASHISH SRIVASTAVA AND S. BRUCE THOMSON

INTRODUCTION

The People's Republic of China (China) has one of the fastest growing economies in the world. For the last 27 years, it has experienced an average yearly economic growth of over 9% (Liu and Li 2002, Morrison 2006, Zeng and Williamson 2003). Therefore, unsurprisingly, it also has one of the fastest growing Internet populations. Even with a 9% penetration rate, it still ranks second in the world in terms of number of Internet users (CNNIC 2006). According to the China Internet Network Information Center, the government agency monitoring Internet use, there were nearly 123 million users in China in 2005 (CNNIC 2006). The improved infrastructure and the growing interest in the Internet represent a phenomenal potential market for e-businesses to tap into. However, this may present a host of social, legal, and political challenges to the Chinese government in seeking to protect individuals and businesses while maintaining socialist ideals.

The Chinese government has worked hard to provide an appealing investment environment to attract foreign investors. The approach since 1979, when it moved from a closed market system to an open market system, has been a carefully orchestrated plan that has suffered relatively few glitches. The initial foreign direct investment (FDI) into China was almost negligible at $109 million (Wei and Lui 2001). In contrast, in 2005, China attracted over $60 billion in FDI (Jiang 2006). Since 1979, over $618 billion has poured into the Chinese economy. This is clearly reflected in improved infrastructure, privatization of businesses, and increased per capita income, which has risen from $290 per year in 1979 to $1260 per year in 2004 (DIS/MOEA 2006, Zeng and Williamson 2003). Although tempered by inflation, this increase in per capita income still represents a considerable increase in disposable income. This adds to the appeal of China's potential e-business market.

To attract foreign investment from individuals, industries and governments, the Chinese government deemed it necessary to institute a series of policies, regulations, and laws. Sweeping reforms were made to labor laws, ownership laws, import/export regulations, tax policies, and communication policies and regulations (Wei and Lui 2001). The primary objective of these reforms was to demonstrate economic and political stability, and thus encourage FDI. China also demonstrated its drive to create an appealing investment environment to attract foreign investors.
economic and political stability by joining the World Trade Organization (WTO). To join, China had to institute reforms as mandated by the WTO (Zhu and Warner 2005). With growing economic activity, the use of the Internet surged. In order to provide a stable and safe e-environment, the Chinese government started monitoring Internet usage; in 2004, it introduced legislation to protect users.

The electronic signatures law was formulated to provide guidelines and protection for e-businesses and their customers. The law illustrates the Chinese government’s endeavor to promote e-business and create an environment conducive to increased international trade and investment. This paper initially provides a brief background to the signature law of China, leading into a discussion of the law itself, which is an example of the Chinese government’s e-business policy. This is followed by the examining the strengths and weaknesses of the electronic signatures law for e-business. In this section, certain key areas of concern for businesses will also be highlighted with recommendations to the business community on how to minimize such problems. The paper ends with a brief conclusion.

THE SIGNATURE LAW OF CHINA – BACKGROUND

Traditionally, a signature is ‘the name of a person written with his or her own hand’ (Merriam-Webster Online Dictionary 2006). This form of signature has been used since the late Roman Empire to authenticate wills (Nicholas 1962). However, no jurisdiction, whether in civil or common law, provides a comprehensive legal definition of a signature (Reed 2000). Civil law countries such as China do not give as much importance to the functions of a signature as common law countries do; rather, they emphasize its form. For example, in common law countries such as the UK and the USA, a person’s name is not the only form of signature. Courts have accepted various other forms of signature such as initials, marks, rubber stamps, typed names, and printed names (Mason 2006). These legally variant forms of the signature indicate that its validity is not to be tested by its form, but rather by the functions it performs (Reed 2000). The primary functions of a signature are to provide evidence: (1) of the identity of the signatory; (2) that the signatory intended the signature to be his or her signature; and (3) that the signatory approves and adopts the contents of the document as his or her own (Reed 2000). Civil law countries such as China emphasize the form of a signature. Only handwritten signatures and seals are legally valid in China (Wang 2006).

As handwritten signatures and seals are the only legally valid forms of signature in China that can be used in the off-line world, the question arises, what form of signature should businesses in China use for online contracts? However, before we answer this question, it is important to examine whether contracts and agreements in China require a signature at all. The contract law (CCL) of the People’s Republic of China states that transactions do not require a signature or a written form unless otherwise stated in the relevant law. The CCL does extend its scope to electronic commerce in Article 11, which states that ‘writing means a memorandum of contract, letter or electronic message (including telegram, telex, facsimile, electronic data exchange and electronic mail), etc., which is capable of expressing its contents in a tangible form.’ The CCL equates the traditional written form to an electronic message, but the law failed to state what technology is equivalent to a handwritten signature or seal in the electronic environment. There is also no mention in the CCL of how the postal rule of contract becomes applicable in the online environment. With China showing great potential for e-business activity, the flaws in the existing law supplied enough impetus to the Chinese government to pursue new electronic signature legislation.

THE NEW ELECTRONIC SIGNATURE LAW OF CHINA EXPLAINED

E-signature, data message, and e-transactions

To address issues regarding an alternative technology to the handwritten signature or the seal, as well as the postal rule of contracts in the online environment, China passed the electronic signatures law (herein after referred to as the Act) in August 2004, which became effective on 1 April 2005. Unlike the CCL, the Act does not use the term ‘electronic message’, but rather the term ‘data message’. It defines data message as ‘information that is generated, sent, received, or stored in electronic, optical, magnetic or other similar form’ (Article 2). The Act defines ‘electronic signature’ as ‘data in electronic form contained in or attached to a data message and that is used to identify the signatory and indicate his endorsement of the contents of such document’ (Article 3). It is interesting to note that although China is governed by civil law, the Act, while defining electronic signature, emphasizes the functions of a signature as in common law countries. It makes no reference, and gives no preference, to any form of technology. Perhaps the reason for this is China’s burgeoning international trade. By emphasizing the functions rather than the form, China harmonized the law with the laws of its trading partners, which include many common law countries. This conforms to Braley’s (2001) view that countries should make their electronic signature laws as easy and harmonious as possible for e-commerce to succeed internationally.

The Act states that only when both parties to the contract and/or other documents agree to the use of
electronic signatures and data messages can this form of signature be used (Article 3). In other words, businesses cannot force their trading partner to use electronic signatures or data messages. Nonetheless, once parties agree to use electronic signatures with data messages, they cannot deny the legal validity of the documents by claiming the absence of a signature in the traditional sense. However, the Act is silent on whether the legal validity of a document with an electronic signature can be disputed by a third party. Can an individual other than the sender and the recipient, or a court or tribunal, deny the validity of a document or a contract sealed with an electronic signature?

Whether in China or anywhere in the world, the provision with regard to what an electronic signature is and when it can be used, is not adequate to persuade a business to enter into e-contracts with electronic signatures. Businesses need to be assured that an electronic signature on an electronic contract is valid in a court of law. In this respect, the Act states that data messages are admissible as evidence in Articles 7 and 8, both of which deal with evidentiary issues associated with data messages. The Act says that the legal requirements of a written form in the off-line world are fulfilled in the electronic environment through the use of a data message, provided the contents of that data message can be exhibited in a tangible form, and that it can ‘be accessed, consulted and used at any time’ (Article 4). In regard to the legal requirement of an original, the requirement is satisfied in the electronic environment by a data message if it can ‘reliably ensure that its contents have maintained their integrity without modification since its finalization’ (Article 5). Any change of form in the course of data exchange, storage, or display is deemed immaterial, provided that the contents maintain their integrity. The Act also talks about document preservation (Article 6). Where the law or regulation requires document preservation, that requirement is fulfilled by a data message if it can satisfy the following two other requirements. First, its format must be identical at the time of creation, sending, and receipt; or, if the format is changed at any stage, its content should accurately reflect the original. Second, the data message should identify its sender and recipient and the time of sending and receiving it.

Other than what forms of electronic signature are acceptable and the admissibility of e-contracts in evidence, businesses in China also need to know when a transaction is considered sent, received, and performed in the eyes of law. This will determine its contractual and legal obligations, because electronic signatures, unlike handwritten signatures, are not attached to a particular individual. An electronic signature is like a seal (e.g., personal identification number (PIN)) that can be used on someone’s behalf with or without the authorization of that person. In such circumstances, does the person whose electronic signature has been used become legally bound by the application of his or her electronic signature? According to the Act, a data message shall be deemed to be sent by the sender if the sending was authorized by the sender (Article 9, Section 1). However, it does not matter whether the sending has been done ‘automatically by the sender’s information system’ (Article 9, Section 2), or whether ‘after verification by the recipient using the method approved by the sender, the results are consistent’ (Article 9, Section 3). This means that if, say, a managing director has given his/her electronic signature to a secretary to use on a relevant electronic transaction or has set up software that automatically affixes that electronic signature, then, in either scenario, that electronic transaction is valid in Chinese law.

Electronic signatures provide businesses with the convenience of entering into legally valid e-contracts without face-to-face meetings of executives of the signing parties. Such e-contracts can be considered analogous to a paper-based contract between two businesses where the contracts are exchanged for signatures through the postal service. The Act provides detailed provisions on how the postal rule of the law of contract is applicable to electronic transactions. It states that when the data message leaves the information system of the sender and enters ‘another information system’ the data message shall be deemed to have been sent. It is to be noted that ‘another information system’ may or may not be that of the recipient. For example, the time at which an e-contract with an electronic signature leaves the sender’s computer and resides on an intermediary server is considered as the time the data message is sent. Similarly, with the receipt of a data message, the Act states that where a recipient has designated a specific system to the sender for sending the data message, the time at which the data message enters the specific system shall be deemed to be the time of the receipt of the data message (Article 11). However, if the recipient has not designated any such system, the time of receipt shall be the time when the data message first enters any of the recipient’s information systems.

Medium-to-large businesses, including those in China, generally have more than one office. It is important for any managers to know where the principal place of business of their business partners is located so that documents sent and received are treated in the eyes of law as legally sent and received. This becomes more complicated with electronic communications because the sender is often unaware of which of the receiver’s specific office systems or servers has received the data message. To address this problem, the Act also deals with the principal place of business of the sender and the recipient. The place where the data message is sent or received shall be considered the principal place of business (Article 12). However, if there is no principal place of business, the sender’s and recipient’s usual place of residence shall be so considered. Both Articles 11 and
12 provide a superseding clause that the parties may agree otherwise on the place of sending and receipt of data message. In such a case, the agreement will prevail over the provisions of Articles 11 and 12.

It is important to note that apart from defining electronic signature the Act also defines ‘reliable electronic signature’ (RES). In other words, there are two types of electronic signatures. One can be considered the standard electronic signature as previously defined. The other is RES, the definition of which is similar to Article 6 of the UNCTRAL Model Law on Electronic Signatures 2001 and the term ‘advanced electronic signature’ used by the European Union Directive 1999. It is important to mention that in all these statutes, whether the term used is ‘advanced electronic signature’ or ‘RES’, the reference is to the technology of digital signatures. Under the Act, an electronic signature satisfies the RES requirements by meeting the following four conditions:

1. At the time the electronic signature creation data\(^2\) are used for an electronic signature, they are proprietary to the electronic signatory.
2. At the time of signing, the electronic signature creation data are controlled solely by the electronic signatory.
3. Any change to the electronic signature after signing can be noticed.
4. Any change to the content and form of the data message after signing can be noticed (Article 13).

Article 14 of the Act states that a RES shall have the same legal validity and effect as a ‘handwritten signature or an affixed seal’ (Article 14). It is important to note at this juncture that if the drafters of the Act had confined it to the traditional concept of a signature in China, RES would have been the alternative form to a handwritten signature or to an affixed seal in the electronic environment. However, China preferred to follow the more open common law approach in this regard and, perhaps, rightly so. The Internet has no territorial boundaries; thus, neither should the regulations governing it. China has aimed to maintain an open approach by adopting a liberal definition of electronic signature.

Furthermore, if Article 14 is read in conjunction with Article 3, it can be inferred that if a non-RES is affixed to a data message, that data message and electronic signature can be denied legal validity by persons other than the creator and recipient. However, in circumstances when a RES has been used in accordance with the provisions of Article 14, its validity cannot be denied legally by either its sender or recipient, or by courts, tribunals, or other third parties that may have an interest in such electronic signatures.

RES or digital signatures are issued by a government-sanctioned body called the Electronic Certification Service Provider (ECSP), which is known elsewhere as a certification authority. With the growing amount of identity fraud, it is important to ensure that applicants are genuine and are not using fabricated documents. Thus, when applying to an ECSP, an applicant must provide true, complete, and accurate information, and ECSPs shall check the applicant’s identity and other relevant materials (Article 20). Applicants who fail to furnish correct information or provide false information to ECSPs shall be liable for any damage caused by their actions (Article 27). However, the Act does not mention the manner in which ECSPs should check an applicant’s identity. Once the identification is verified by ECSPs, they will provide electronic signature creation data, electronic signature verification data (private key and public key in case of digital signatures), and the electronic signature certificate to applicants, which can be used for entering into legally valid transactions.

E-contracts with businesses outside China

The Act provides for the legal recognition of electronic signature certificates issued by ECSPs outside China (Article 26). It states that where the State Council Department in charge of information industry has given an approval after a relevant agreement or where there is a principle of reciprocity, electronic signature certificates issued by ECSPs outside China shall be legally valid within China. It means that, for example, the State Council Department in charge of information industry has a reciprocity agreement with India’s Controller of Certifying Authorities, electronic signatures issued by ECSPs/certification authorities in India will be recognized in China, and vice versa.

Security of electronic signatures

As mentioned above, electronic signatures, unlike handwritten signatures, are not attached to a particular individual but are like a seal that can be used on someone else’s behalf – with or without the authority of that person. In such circumstances, persons whose electronic signature has been used can be legally bound by any application of their electronic signature. The Act therefore obliges the electronic signatories, especially in the case of the RES, to secure their electronic signature creation data (Article 15). It states that an ‘electronic signatory shall duly safeguard his electronic signature creation data’ (Article 15). The moment they realize that such data have been descrambled or may have been descrambled, they should inform the relevant parties and stop using the signature. An electronic signatory shall be liable for damages for the misuse of his electronic signature creation data (private key in case of digital signatures) even if he is not at fault (Article 15). The Act does provide protection to prevent the fraudulent use of electronic signatures. It states that if anyone forges,
fraudulently uses, or misappropriates a third party’s electronic signature, a criminal or civil action can be taken against that person depending upon whether the act constitutes a criminal offense or causes loss to the third party (Article 32).

**STRENGTHS AND WEAKNESSES OF THE ACT**

One of the Act’s strong points is that it is not technology-specific but rather technology-neutral. It thus allows technological advances without requiring any amendment to the provisions of the Act. Therefore, even if a new form of electronic signature is developed, the law would remain the same and would apply to the new technology. Moreover, the Act is quite thorough on how contractual requirements are satisfied in the online environment, and it clearly defines terms such as ‘data message’, ‘electronic signature’, and ‘RES’. As a further example of flexibility, the concept of the postal rule of the law has been carefully extended to the online environment. An electronic transaction is deemed to be sent when it leaves the sender’s computer and is deemed to be received when it enters the receiver’s designated system.

Despite these strengths in terms of flexibility and openness, the Act does display some weaknesses. The procedure to obtain an RES has no guidelines on what constitutes valid and invalid identification. Under the current regulations, what is acceptable as valid identification may vary according to the ECSP office from province to province, city to city, and perhaps even from office to office within the city. The Chinese government needs to establish a stringent set of identification guidelines. This will create a higher level of confidence in the users of ECSP services, in turn generating higher levels of trust for parties entering into online contracts.

A second area of concern relates to the liability of electronic signature/RES users. Currently, the law stipulates that the user is liable for any damages/costs caused through the misuse of an electronic signature/RES regardless of due diligence. Since the Internet is an insecure network, any electronic signature creation data, such as a private key, can be descrambled without any intentional wrongdoing or negligence on the part of the electronic signatory (Srivastava 2005). This particular aspect was considered by legislators in Switzerland when drafting their electronic signature law. According to Switzerland’s electronic signature law that took effect 1 January 2005, electronic signatories are not liable for the misuse of their electronic signatures if they can prove that they had taken adequate precautions and were not at fault. However, this does highlight security as a key area of concern for businesses.

In order to prevent the misuse of their electronic signatures, especially the electronic signature creation data (private key in case of digital signatures), businesses in China should make sure that the electronic signature creation data used for the creation of a RES is kept in a secure location. If these data are stored on the hard disk of the office computer, they must be secured not only through a password but also by the physical security of that hard disk. For example, the computer’s hard disk containing the data should be kept behind locked doors with access only to those authorized by the company to use the RES. Such precautions will prevent unauthorized employees from fraudulently using the company’s RES. Businesses should also ensure that a corded, not wireless, keyboards are used with RESs as a precaution. Wireless keyboards may be insecure because the keystrokes of the user of RES may be transmitted to another person’s computer in the same office or to another computer some distance away (Brandt 2003).

It is recommended that businesses should refrain from storing their electronic signature creation data on the hard disk of a computer, because most computers, especially those in workplaces, are connected to the Internet or an intranet, and hence are prone to online/external attacks (Srivastava 2005). Organizations should store their electronic signature creation data on portable information storage devices (PISD), such as a smart card or a flash disk, secured by a PIN or password. Storage on such devices minimizes the problem of online attacks; however, users should take care not to leave the PISD in the workstation unattended.

The shortcoming of using PISDs is that subscribers can lose their PISD, and the finder may be able to open the subscriber’s electronic signature creation data with malicious intent. This drawback is similar to that associated with bank cards. However, the success of bank cards indicates that this shortcoming is not likely to influence the acceptance rate of RES embedded on a PISD. A strong advantage of storing the electronic signature creation data on a PISD is that it gives the convenience of signing through one’s RES from any computer terminal anywhere in the world. Therefore, by following basic guidelines, businesses that use RESs may significantly reduce the risk of misuse.

**CONCLUSION**

This paper has discussed the electronic signatures law and whether or not it meets the requirements of the e-business challenges in China. It appears that China has created an electronic signature law that recognizes and provides support for businesses to cultivate the open, flexible, and ever-changing e-environment. The strength of the Act is that it provides a basis for how contractual requirements are satisfied in the online environment. The concept of a ‘signature’ and the postal rule of the law have been carefully extended to cyberspace. However, the Act is also characterized by a few weaknesses essentially related to identification guidelines.
and the liability of electronic signatures/RES users. As a result, the Act has failed to create an atmosphere of confidence and trust for parties willing to enter into online contracts. To overcome these weaknesses, the Chinese government needs to devise a set of appropriate guidelines for identification and liability. Security as a key area of concern for businesses was also highlighted. Recommendations have been made regarding measures businesses should take to minimize these concerns and protect themselves from the misuse of their electronic signature/RES.

Overall, China’s electronic signature law warrants a cautious seal of approval. The prognosis for e-business in China looks healthy. The government, through its regulations and policies, seems determined to create an environment that allows businesses to pursue e-business domestically and internationally. The electronic signature law is an initial step to a sound basis of trust in online contracts, and it should promote further investment in China and encourage Chinese investors to seek international investments.

Notes
1. Hong Kong and Macao are treated as separate entities by the Chinese government under a ‘one country, two systems’ approach (Cai 1999); therefore, when referring to China, this paper will exclude Hong Kong, Macao, and Taiwan.
2. In the context of digital signatures, the ‘electronic signature creation data’ will be the private key of the signatory.

References