Law of Electronic Commercial Transactions

Contemporary issues in the EU, US and China

Faye Fangfei Wang

Routledge Research in IT and E-Commerce Law

Part III

Online security

7 Electronic signatures

In practice parties involved in electronic commerce in open networks such as the internet are faced with the problem of the identity of the communicating parties, i.e. knowing that the sender of an electronic message is actually the person they claim to be. In addition, communicating parties also need to ensure that the electronic message received is the one that was actually sent, i.e. the integrity of the message.[1] A signature is a familiar way for individuals to make apparent on paper that they are who they say they are and that, often, they agree to be bound by whatever they are signing. A signature, therefore, generally provides authentication of the signatory. It is also an indication of 'acceptance' or 'consent' to a legally binding commitment.[2]

In the new era of the information society the ultimate medium of remote communication between unknown parties is established on the internet.[3] E-transaction security becomes a significant barrier to the development of e-commerce. Many websites use a technology called Secure Sockets Layer (SSL) to encrypt personal information over the internet. To ensure that an e-transaction is safe customers usually look for the logos of the companies, such as VeriSign or TrustE.[4] Thus, as a result of technology shift from traditional face-to-face transactions, technical architectures and authentication methodologies often substitute for the trust that trading partners formerly developed between each other.[5] Identification and authentication provides senders and receivers with assurances that each party will be identified uniquely so that each will know where transactional information originated from and to whom it was sent.[6]

From a legal perspective businesses may be reluctant to get involved in an electronic transaction if the present legal framework fails to offer necessary guarantees for a trustworthy and secure online commerce. But these goals can be achieved through the use of electronic signatures. For electronic signatures to accomplish such objectives in open networks they need to be used in conjunction with certificates issued by certification service providers (CSPs), which certify the veracity of the link between the electronic signature and the identity of the electronic signature holder. Therefore, for electronic commerce to flourish, electronic signatures must be legally recognised as equivalent to their hand-written counterparts. In addition, a legal regime must be set up for

the establishment and functioning of certification service providers which can generate trust among trading parties in certification authorities (CAs), and thereby in electronic signatures. Further, the security issues need to be addressed, not only on a national level but also and most importantly internationally, in order for e-commerce to blossom.[7] One of the major legal challenges is recognition of foreign electronic signatures and authentication as the new technology encourages transnational transactions.

This chapter will firstly attempt to look at the definitions, features, benefits and functions of electronic signatures and electronic authentication, analyse the different types of electronic signatures available in the market and, in particular, highlight digital signatures – one of the most important forms of electronic signatures – using cryptography technology. Secondly, this chapter will identify the forms and conditions of establishing Trusted Third Parties, called Certification Authorities (CAs) providing electronic signatures and authentication services. Thirdly, the chapter will focus on one of the legal aspects uniquely connected with electronic signatures, i.e. the duties and liabilities of CAs, especially on the liability regime which applies between CA and a third party who uses the certificate to validate the identity of a certificate holder intending to transact with the third party. Fourthly, this chapter will critically analyse and compare the EC Directive on Electronic Signatures,[8] the US Uniform Electronic Transactions Act (UETA),[9] the US Electronic Signatures in Global and National Commerce Act 2000 (ESIGN Act)[10] and the Law of People's Republic of China on Electronic Signatures (China Electronic Signatures law),[11] alongside an examination of the international laws, UNCITRAL Model Law on Electronic Commerce, UNCITRAL Model Law on Electronic Signatures and UN Convention on the Use of Electronic Communications on Electronic Contracting (the UN Convention).[12] Finally, this chapter will provide suggestions concerning the international harmonisation of electronic signatures legislation, as well as the possibility of the achievement of a common global consensus on electronic authentication.

7.1 Current legislation: EU, US and China

It has been widely accepted that it is necessary to provide evidence of a party's intention to be bound by a contract by making a written signature. That is to say, the evidence of transactions usually derives from the paper-based contract, which is finalised by a manuscript signature. In *Goodman v J Eban Ltd* it outlines a general principle: 'the essential requirement of signing is the affixing in some way, whether by writing with a pen or pencil or by otherwise impressing upon the document, one's name or "signature" so as personally to authenticate the document'.[13] A signature enclosed electronically should be treated as 'most closely analogous to a rubber stamp signature'.[14] In the modern information world, using electronic means to sign one's name should be acceptable in the same way as a written signature. However, unlike individual manuscript signatures, electronic signatures lack the uniqueness in written

pattern. These identified limitations necessitate electronic documents to prove trustworthiness and authenticity.[15] So how can it be done?

Electronic signatures should be the key point in this authentication process. At the international level, according to Article 2 of the UNCITRAL Model Law on Electronic Signatures 2001, an 'electronic signature' means 'data in electronic form in, affixed to or logically associated with, a data message and to indicate the signatory's approval of the information contained in the data message'.[16] Article 6 sets out the features of an electronic signature, which are: '(a) it is uniquely linked to the signatory; (b) it was created under the control of the signatory; (c) its integrity is clear; and (d) the integrity of the message is also clear from signature'.

The EC Directive on Electronic Signatures defines an electronic signature as 'data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication'.[17] In the US, the Uniform Electronic Transactions Act (UETA) simply allows the signature to be accomplished through electronic means. There are no specific requirements of technology to be used in order to create a valid signature.[18] For instance, one's voice on an answering machine may suffice if the requisite intention is present. Similarly, including one's name as part of an electronic mail communication also may suffice, as may the firm name on a facsimile. Therefore, a symbol, sound or process would not amount to a signature in the absence of the requisite intent. In electronic communication one may use a digital signature with the requisite intention, or one may use the private key solely as an access device with no intention to sign or accomplish a legally binding act. In any case the critical element is the intention to execute or adopt the sound or symbol or process for the purpose of signing the related record. Under the US ESIGN Act, an 'electronic signature' is widely defined as 'an electronic sound, symbol or process, attached to or logically associated with a contract'.[19] In China, the China Electronic Signatures Law defines an 'electronic signature' as 'data included and attached in data message in electronic form, for the use of identifying the identity of the signatory and showing that the signatory has recognized the contents therein'.[20]

As noted above, although there are different definitions in different laws, the effectiveness of an electronic signature should be the same: an e-signature is only producible by the sender and any change will make it incompatible with the integrity of the signature. Parties must be able to use techniques to ensure that the business conducted over the networks will be secure. Briefly speaking, electronic signatures should be regarded as a means of verifying the identity of the user of a computer system to control access or authorise a transaction.

7.2 Forms of electronic signatures

Electronic signatures can take many forms and can be created by many different technologies. Currently the forms of electronic signatures include,

but are not limited to, password or personal identification number (PIN); email signatures; smart card;[21] biometrics;[22] scanned signatures and digital signatures. On a daily basis the most common forms of electronic signatures are PIN, scanned signatures, email signatures and digital signatures.

7.2.1 Word documented or picture-scanned signatures

There is a feature in Microsoft Word which allows users to add a password to protect word documents. The password added to the word documents is known as a word documented signature. Such a password is also called 'personal identification number (PIN)'. It is a set of numbers or characters generated and shared between the system and the user. This is one of the basic forms of electronic signatures.

Picture-scanned signatures are also very common. Instead of signing a piece of paper manually using a pen, a device with scanning technique allows users to scan such a piece of paper with a handwritten signature into the computer thereby creating an electronic 'bitmap' or 'JPEG' image of the signature. The digital image file could then be attached to the document file as an electronic signature. It is convenient and less costly to use picture-scanned signatures, however such files are very easy to forge as much less skill and effort is required to simply scan a piece of paper.

7.2.2 Email signatures

An email signature can consist of text or pictures, or both. Most of the email portals have a tool for users to create and use a signature. For example, Microsoft Outlook automatically adds the created text or pictures as a signature to the users' outgoing email messages. In recent years more and more email signatures software has been launched to help users develop a more secure email signature, for example, 'signature creator I software' helps creating 'handwriting' signs to accent the users' individuality of signatures in email messages (see Figure 7.1 opposite).

However, the UNICTRAL Report on Promoting Confidence in Electronic Commerce in 2007 states that 'neither typed names on unencrypted email messages nor scanned signatures offer a high level of security or can definitely prove the identity of the originator of the electronic communication in which they appear. Nevertheless, business entities freely choose to use these forms of "authentication" in the interest of ease, expediency and cost-effectiveness of communications'.[24]

7.2.3 Digital signatures

A digital signature is one of the most important and reliable forms of electronic signatures. It is defined in the ABA's (the American Bar Association) Guidelines as 'a transformation of a message using an asymmetric

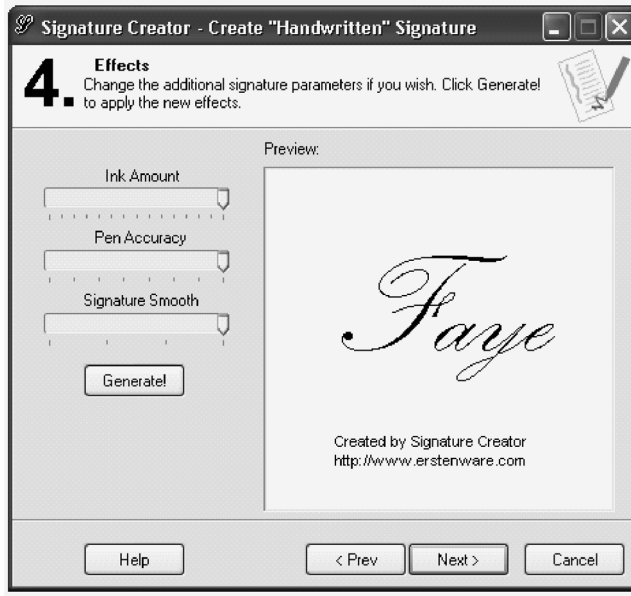

Figure 7.1 Signature Creator 1.12 description.[23]

crypto-system and a hash function such that a person having the initial message and the signer's public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key, and whether the initial message has been altered since the transformation was made'.[25] Digital signatures are generated through cryptography (i.e. encryption and decryption techniques).[26]

So what is cryptography?

Cryptography can be defined as an act of secret writing composed of a series of ciphers and codes used to hide a message's content. In effect, the message will become impossible to read when parties do not have the code to decrypt it.[27] There are two types of cryptographies: the first one, known as symmetric or secret key cryptography, uses the same single key for the encryption and decryption process. The second one is called asymmetric or public key cryptography and utilises two different keys for the encryption and decryption process.[28] Asymmetric or public key cryptography is widely used in electronic signatures nowadays: a private key (held only by the sender of transmitted data) is used in conjunction with a signature algorithm to sign the data, and a public key (often made public in an online directory) is used by the recipient of the data with the algorithm to verify the signature received. For example, assume that A is a sender and B is a receiver. A would like to communicate with B, a stranger with whom A has never communicated before, A and B could exchange the plain text of their public keys. Then, A and B can each encrypt their outgoing messages with the other's

public key and decrypt their received messages with their own secret, private key. Then again, there may be a problem: how could A know whether the message was really from B or from an impersonator? B may have the same problem regarding A. So it needs a trusted party, such as a Certification Authority (CA), to make a confirmation of their public keys as well as the accuracy of the information by issuing certificates to both parties. With the CA's guarantee digital signatures will come into legal effect.

As stated above, digital signatures are based on what is technically known as dual key cryptography. When an electronic signature is created two 'keys' are created with it: a private key and a public key. These keys are mathematical codes that are different from each other, but inextricably linked. The private key remains with the person who owns the electronic signature and is kept secret, whereas the public key is distributed freely. The relevance of these keys to an electronic signature is best explained by way of an example.

Suppose that A wishes to send B an email, preferring to sign electronically. A could compose the email and electronically sign it by attaching his digital certificate as well as his public key. When A sends the email his private key encrypts his signature. When the email is received, B will use A's public key to decode the encrypted signature. Once the signature has been unencrypted, B will be able to confirm that it was A who sent the email. This confirmation process is known as authentication.[29] If, therefore, A accepted an offer by B, then the use of his electronic signature would be the same as signing a contract manually.

7.3 Benefits

There are two major benefits that can be identified with the use of electronic signatures. The first is that when an electronic signature is used and the authentication process has been completed the recipient of the email will be informed as to whether the email has been tampered with during the process from the sender's computer to the recipient's computer. As a document is digitally signed the private key will perform a mathematical calculation of the entire contents of the document. This will produce a summary which is also encrypted and sent along with the document. When the document reaches the recipient's computer and the public key is authenticating the signature the public key will perform a similar calculation of the document's contents and also produce a summary. The mathematical link between the two keys means that the summaries will be identical if the document received is exactly the same as the document that is sent. The first summary (created by the private key) is unencrypted and then compared with the new summary (created by the public key) and if one is different from the other, the recipient is notified that the document has been intercepted and altered en route. Although occurrences of 'email hijacking' are low, given the number of emails that are sent each day, the value of some property transactions could make attempts at email interception and tampering attractive.

The second benefit of electronic signatures is that they allow for the transmission and receipt of secure emails. This is a highly desirable property, especially for lawyers who will often have to deal with highly sensitive and confidential information. Secure emails become possible once one person has another person's public key. Although in the example given above the public key accompanies the electronic signature, this does not need to be the case. The public key can be emailed separately to an individual; copied to a disk and sent through the post; or even downloaded from a dedicated website.[30]

An example of the digital signature process is: if A wishes to send B a secure email, A will use B's public key to encrypt the email and also any documents that are attached. Once encrypted the only way that the email can be unencrypted is with a public key's corresponding private key. Therefore, if A's public key has encrypted the email it can only be unencrypted by A's private key. If anyone intercepts the email whilst in transit, they will be unable to view its contents unless they have a copy of A's private key.[31]

7.4 Functions

Digital signatures can be deemed to be the process of creating, using and verifying a signature, and they provide important functions for legal purposes.[32] Firstly, the asymmetric cryptography – PKI – ensures a high level of security in e-communications and of confidentiality of the context of a message sent over an open network like the internet. Secondly, digital signatures provide authentication of the identity of the signer by attributing the message to the signer; so it is known who participated in a transaction. The rationale of this function is based on the fact that digital signatures cannot easily be forged unless the signer loses control of this private key either accidentally or intentionally. Thirdly, the digital signature protects the integrity of the transmitted data so the recipient can be sure that comparing the two message digests will not have altered the message.[33]

In short, digital signatures accompanied by an electronic certificate can provide three important functions: (1) authentication, which is to authenticate the identity of the person who signed the data so it is known who participated in the transaction; (2) integrity, which is to protect the integrity of data so it is possible to know the message read has not been changed, either accidentally or maliciously; and (3) non-repudiation, which is to allow it to enable it to prove subsequently who was involved in a transaction, thus preventing anyone from denying that he sent or received the data. Therefore, documents that are authenticated by a secure electronic signature are entitled to a presumption of integrity, that the signature is that of the person with whom it is associated and that the user affixed the signature with the intent of signing or approving the document.[34]

When transactions involve several stages in different time, consistency of identity is more difficult to prove. For example, how can it be proved who

participated in the particular transaction? What will make the identity of the sender and recipient of the data undeniable? How can one establish who else might have read this message? Does the sender have the authority to do this transaction? What happens if the decryption key is lost? Who is liable if the decryption key is compromised?[35]

Under those circumstances verification plays a central role in the process of establishing identity within a PKI.[36] To verify a digital signature the verifier must have access to the signer's public key and have assurance that it matches the signer's private key. As it is merely a pair of numbers a public and private key pair has no inbuilt connection with any person. For the purpose of security persons who are not previously acquainted, but who wish to transact with one another via computer networks such as the internet, will need a means of identifying or authenticating each other. It is necessary to use one or more trusted third parties to associate an identified signer with a specific public key to build up a bilateral relationship. The third party, a Certification Authority (CA), can vouch for a party by issuing a certificate identifying him/her, or attesting that he/she possesses a necessary qualification or attribute. Thus, it establishes trust in the electronic transaction.

7.5 Legal recognition

Traditionally, to qualify as a valid and effective signature, four evidential requirements shall be fulfilled:

1 the intention of signing;
2 the identification of a signed person;
3 the authorisation of signing; and
4 the integrity and originality of a signature.

To qualify a valid and effective electronic signature the four evidential requirements in a written signature above shall also be fulfilled. In general, Article 9 of the UN Convention on the Use of Electronic Communications on International Contracts (the UN Convention)[37] deals with electronic functional equivalents for writing, handwritten signatures and originals. Article 9(3) of the UN Convention contains a new rule for the electronic functional equivalent of a handwritten signature. Article 9(3)(a) provides that the conditions for electronic signatures to be equivalent to handwritten ones will be if 'a method is used to identify the party and to indicate that party's intention in respect of the information contained in the electronic communication'. The expression of 'party's intention' used in the UN Convention is different from the analogous provision in the UNCITRAL Model Law on Electronic Commerce, which refers to the phrase 'party's approval of the information contained'.[38] It is a significant improvement in that it emphasises the identity of the party and his intention for the information,[39] whilst the UNCITRAL Model Law on Electronic Signatures and the UNCITRAL

Model Law on Electronic Commerce require 'the integrity of the information which it relates'.[40]

But the UN Convention is silent on what constitutes a valid electronic signature. Can a typed name in the context of an email form a valid signature? What are the recognised standards of e-signature techniques?

In the recent case *Mehta v JPF*,[41] Mr Mehta was a director of Bedcare (UK) Ltd. Bedcare failed to pay the supplier, J Pereira Fernandes (JPF) and was ultimately wound up on a petition by JPF. The case was about the defendant Mr Mehta who asked a member of his staff to send an email to JPF's solicitors for personal guarantee. The email was not signed by Mr Mehta but is described in the header as having come from Nelmehta@aol.com. The two key issues at the hearing of the appeal were:

(1) whether the email constituted a sufficient note or memorandum of the alleged agreement for the purposes of section 4 of the Statute of Frauds[42]; and
(2) assuming the email was a sufficient note or memorandum, whether it was sufficiently signed by or on behalf of Mr Mehta, it being contended on behalf of JPF that the presence of the email address on the copy of the email received by JPF's solicitors was a sufficient signature for these purposes.[43]

So the focal points here are whether the email was sufficient memorandum or note, and whether the sender's automatically inserted email address can constitute a signature.

Judge Pelling QC held that the email was indeed a note or memorandum because the email was in writing and it was not disputed by Mr Mehta that the offer was orally accepted by JPF.[44] As the defendant's name or initials did not appear at the end of the email or in the body of the email, the judge considered the issue here to be whether a note or memorandum has been signed at all, rather than with what intention or with what capacity Mr Mehta or his employee signed the relevant document.[45] Thus, the judge concluded that the presence of the email address at the top of the email did not constitute a signature, following the ruling of *Evans v Hoare*,[46] stating: 'whether the name occurs in the body of the memorandum, or at the beginning, or at the end, if it is intended for a signature there is a memorandum of the agreement within the meaning of the statute'.[47] The judge regarded the inclusion of an email address in such circumstances as a clear example of the incidental inclusion of a name in the absence of a contrary intention.[48] However, if a party or a party's agent sends an email and types his or his principal's name to the extent required or permitted by existing case law in the body of an email, then it would be a sufficient signature for the purposes of section 4 of the Statute of Frauds.[49]

In practice it is extremely difficult to detect fraudulent emails as attackers have become increasingly sophisticated. Email recipients cannot rely on the

sender's email address to validate the true origin of the email. Unfortunately, while it may look legitimate, the 'From' field can be altered easily.[50] Thus, the debated point of whether an email header can constitute a signature should focus on whether the email system is secure to guarantee that the sender is the one that sends the email, rather than whether the email address itself constitutes a signature. This should be clarified in the relevant future legislation.

Another major issue is whether typed names in emails constitute signatures. In the author's view the concern should focus on the security of the emailing systems, i.e. whether the email systems use secure portals or layers, such as SQL, to verify the identity of the email users, rather than the typed form of names contained in the email. If the emailing system can be proved to be secure there will be sufficient evidence that the email originates from the account owners or authorised users. As a consequence the typed name contained in the bottom of an email as a signature, or even an automated signature which the user creates in a fixed box using the signature button in the email system, will become irrelevant.

The UN Convention has no direct provisions that can be employed, for instance, to the *Mehta* case, but it has included conditions that constitute a presumed valid signature. As for Article 9(3)(b), which prescribes a reliability requirement for the validity of an electronic signature, the UN Convention Working Group had considered two alternative formulations: one is based on Article 7 of the UNCITRAL Model Law on Electronic Commerce; and the other is based on Article 6(3) of the UNCITRAL Model Law on Electronic Signatures.[51] Article 9(3) of the UN Convention provides:

> Where the law requires that a communication or a contract should be signed by a party, or provides consequences for the absence of a signature, that requirement is met in relation to an electronic communication if:
>
> a A method is used to identify the party and to indicate that party's intention in respect of the information contained in the electronic communication; and
> b The method used is either:
>
> i As reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement; or
> ii Proven in fact to have fulfilled the functions described in subparagraph (a) above, by itself or together with further evidence.

In Article 9(3) a legal requirement for a signature is met by an electronic signature if Article 9(3)(a) is satisfied, or, either Article 9(3)(b)(i) or Article 9(3)(b)(ii) is satisfied. Article 9(3)(b)(i) can be deemed as prescribing 'reliability in theory', whereas Article 9(3)(b)(ii) can be regarded as prescribing 'reliability in fact'.[52] In practice the 'exception' in Article 9(b)(ii) is likely to

swallow the original 'rule' in Article 9(3)(b)(i), thereby avoiding the problems associated with Article 9(3)(b)(i). Thus, it is a significant improvement over both Article 7 of the UNCITRAL Model Law on Electronic Commerce as well as Article 6(3) of the UNCITRAL Model Law on Electronic Signatures.[53] However, although Article 9(3)(b) of the UN Convention applies a functional equivalent principle to adopt the new emerging techniques, it doesn't define what standards of techniques are 'as reliable as appropriate' and what are required for further evidence.

Another problematic issue of security is the interaction between the participants. For example, let's imagine a scenario involving a user (as principal), an electronic agent (as agent) and another user (as the third party): the user uses the intelligent agent as his own agent for contracting, the third party enters into the contract-aimed interaction with the agent, without knowing who (what) stands behind the latter. Neither of the users knows with whom his agent interacts. The only link between them is the agent. Consequently, in the case that something went wrong, the third party could not address the user directly, because the electronic agent has not provided the identification of the user. This problem could be solved if the user ratified the actions of the agent, providing in this way his identification to the third party. Another solution, in order to increase the trustworthiness on the use of artificial intelligences, could be the adoption of an agency fiction: if the third party had reasonable cause to believe the agent acted on behalf of the principal, the principal would be liable.[54]

8 Electronic authentication

8.1 What is electronic authentication?

'Authenticate' means, according to the UCITA:

> (a) to sign; or
> (b) with the intent to sign a record, otherwise to execute or adopt an electronic symbol, sound, message, or process referring to, attached to, included in, or logically associated or linked with, that record.[1]

'Authentication' means satisfying the court:

1 A document is relevant;
2 A document serves as a piece of evidence;
3 Such evidenced document is connected with a person, place or thing, or a process.[2]

In most civil law jurisdictions authentication is understood in a narrow scope and a strict way as that the authenticity of a document has been verified and certified by a competent public authority or a notary public.[3]

Electronic authentication can be characterised as the process through which the identity of a computer or network user is verified. Authentication ensures that an individual is, in fact, who he or she claims to be. It is distinct from identification which determines whether an individual is known to the system, and from authorisation, which grants the user access to specific system resources based on identity.[4] In other words, authentication should be a means of providing trustworthy electronic commerce or electronic service delivery, which is used to protect undetected modifications to an electronic document, providing limited, but reliable, information about a person, and providing other functions of a signature in an electronic environment, in particular the signer indicating approval of the signed documents. However, this authentication should comprise a digital signature relying on asymmetric cryptography, the infrastructure for authenticating information about people and systems, and the mechanism for binding a signature to a digital

document.[5] In essence, the most common type of authentication certificate is an identity certificate, widely called a public key certificate (PKC), which has been adopted internationally.

As the purpose of electronic authentication is to confirm the identity of a generator of an electronic document the identity of a subscriber must somehow be confirmed in an electronic authentication system. In short, authentication is a process used to ascertain the identity of a person or the integrity of specific information. For a message, authentication involves ascertaining its source and making sure that it has not been modified or replaced in transit.

8.2 The differences between E-signatures and E-authentication

When conducting electronic commerce certain authentication methods need to identify those parties involved in a transaction or an application. So what are the differences between electronic signatures and electronic authentication?

In the offline environment, authentication and signature do not have the same meaning in different legal systems.[6] Authentication is known as a document or piece of evidence connecting with a person, place or thing.[7] A signature is 'any name or symbol used by a party with the intention of constituting it his signature'.[8] From the author's perspective, electronic signatures focus particularly on verifying the identity of the owners dealing with the problem of documental attribution, while electronic authentication deals with the problem of the reliability of key encryption (i.e. public key and private key) and its key holders.

Certification of an electronic signature could combine the functions of signature and authentication, as this kind of certification requires that 'the person whose signature it is has made a statement confirming that the signature, a means of producing, communicating or verifying the signature, or a procedure applied to the signature is a valid means of establishing the authenticity or the integrity of the communication or data or both'.[9]

8.3 Trusted third parties: Certification Authorities (CAs)

8.3.1 Definition

A certification authority (CA) is a trusted third person or entity that ascertains the identity of a person, called a subscriber, and certifies that the public key or a public-private key pair used to create digital signatures belongs to that person.[10] That is, trusted third parties (TTPs), called certificate authorities (CAs, also sometimes referred to as 'intermediate systems' or 'certifiers'), offer a way to confirm that a public key belongs to the claimed owner in an independent way.[11] The CA does this by issuing a certificate which associates an individual with a particular public encryption key.[12] The certificate

contains the public key and name of the signatory, digitally signed by the CA.[13]

Therefore, to associate a key pair with a prospective signer a certification authority issues a digital certificate which is an electronic record guaranteeing that the prospective signer identified in the certificate holds the corresponding private key. The prospective signer is referred to as the 'subscriber'. A certificate's principal function is to bind a key pair with a particular subscriber. A 'recipient' of the certificate can use the public key listed in the certificate to verify whether the digital signature was genuinely created by the prospective signer holding the corresponding private key.

8.3.2 Requirements

Public key cryptography constitutes an attractive technology but it leaves one major gap: how does one correspondent know whether he has the right key for the other correspondent? Two individuals will be able to communicate in confidence if they have a secure channel over which they can pass a key. This will be achieved, by sealing, for example, a piece of paper or diskette in an envelope and sending it through the mail. But they will not have such a secure channel if they wish to rely simply on electronic media. No one can trust an email message saying 'Here is my public key' because the very message containing that key may have been sent by an eavesdropper. The problem arises whenever two people who do not previously know each other wish to communicate. It often comes to the forefront during online commerce, where a customer wants to get assurances that he can trust someone who is claiming to offer goods and is asking for payment.[14]

Trusted Third Parties (TTPs), such as CAs, may be the solution that allows an initial contract to be made. If you and your desired correspondent both know an intermediary and entrust it with your keys you may decide to obtain each other's public key and start communication. Furthermore, with reference to the functions of digital signatures, the use of this technology for TTPs is currently the most efficient system of establishing a secure and user-friendly environment of e-transactions and reinforcing both business and consumer trust in e-commerce.

Sometimes a trusted third party plays a role as an agent. For example, PayPal, an eBay company, enables any individual or business with an email address to securely, easily and quickly send and receive payments online.[15] Customers who enrol with PayPal only need to provide their account information once. It will then be stored on a secure, highly encrypted server. When purchasing something using PayPal users simply carry out the transaction through their PayPal accounts rather than a credit card. This method is safer, more secure and more convenient than providing financial information to multiple sites of individual sellers.[16]

8.3.3 Functions and roles

As stated above, a certification authority (CA) is a TTP that 'acts as a repository of public keys and authenticates the relationship between a particular public key and its supplier'.[17] A CA can be public or private, which seeks to fill the need for trusted third party services in electronic commerce by issuing electronic certificates, signed electronically, that attest to some fact about the subject of the certificate. However, a certificate should be considered a digitally signed statement by a CA, which provides independent confirmation of an attribute claimed by a person proffering a digital signature.[18] Generally, the certification process requires subscribers to create their own private/public key pair and, after having established their identity to the CA, to demonstrate that they have a private key corresponding to the public key without disclosing the private key.

Once the CA has checked the affiliation between the identified private individual and a public key it will be able to issue a certificate. A certificate is a digital record that guarantees the link between a public key and the subscriber. It contains the subscriber's identity with the public key and the issuing CA's identity with its own digital signature for the authenticity and integrity of the certificate. Before being made public the certificate's content may be reviewed by the subscriber who will thereafter be bound by any document signed with his private key if it corresponds to the certificate's public key.[19]

Once the certificate's accuracy has been confirmed the certificate can be published to make it available to third parties who would like to contact the subscriber. The most frequent online publication for certificates is an electronic database of certificates known as a repository. A repository will also provide additional information on certificates such as their suspension or revocation if the key was lost or compromised. After being published the certificate can be attached to any electronic communication to enable any recipient to check the connection between the public key and the sender. Therefore, the CA ensures the security of digital signatures to be used as authenticating tools and thus plays a principal role in boosting the growth of secure electronic communications.[20] Since the conduct of the CA will affect the normal operation of electronic markets, the regulation of its forms and conditions of establishment is important.

8.3.4 Forms

There are several forms of CAs available in the electronic market. There are certification authorities that are licensed (called recognised certification authorities (RCA)) and some other certification authorities operating under a form of voluntary licensing or accreditation (called a voluntary recognition system of certification authorities). But there is no uniform standardisation in relation to these forms of CA. Most of the developing countries, such as

some Asian countries, impose a mandatory registration system on all CAs, while most of the developed countries, such as the UK and the US, adopt a voluntary recognition system, that is, CAs are free to apply for recognition on a voluntary basis but only those CAs which have achieved certain objective standards will be 'recognised'.[21]

In the US, for example, certification authorities may include federal and state governmental entities, private persons or entities licensed to act as certification authorities by a state, and private persons or entities acting as certification authorities for commercial purposes.

For example, the US Postal Service (USPS) may be suited to function as a certification authority. In transactions between companies or individuals, it can be seen as a reputed, credible objective third party. Furthermore, its nationwide network of post offices enables applicants to appear in person to provide the confirmation that a registered public key corresponds to an actual, real person.[22]

While the apparent assumption in many jurisdictions has been that the government will act as the licensing or accreditation authority (whether as part of a mandatory or voluntary regime), there is growing recognition that private sector organisations, or other types of standards bodies, may be better suited to this role. For example, private entities may also operate as CAs. For example, VeriSign, Inc.,[23] supplies certifications and related digital services to natural and legal persons. Furthermore, the Netherlands has, for instance, set up a voluntary Trusted Third Party Chamber with the aim of bringing together the government and private entities, which would be better equipped to the rapid development of the market and its applied technologies.[24]

However, whether to require licensing of Certification Authorities or, if not, whether to provide some other form of voluntary licensing or accreditation, depends on what would be more suitable to the country's economic foundation, technology facilities, legal environment and governmental policies, since both of them have their own advantages. The main benefit of recognition of a CA is that it will afford significant limitations on its potential legal liabilities. For example, an RCA which has complied with all material requirements will not be liable in case of loss based on a counterfeit digital signature backed up by certificates issued by the RCA. Therefore, to avoid unlimited legal personality CAs should endeavour to become RCAs.[25]

8.3.5 Conditions of establishment

When a CA needs to apply for a licence to engage in an electronic authentication service it must comply with a set of requirements of extremely specific (and generally quite stringent) financial and technical standards, such as subject qualifications, hardware management, software conditions, as well as the capability of compensation and so on. CAs must have sufficient registered share capital and satisfy certain fitness and character requirements. However, the Utah Digital Signature Act firstly sets a good example of conditions for

establishing CAs. Under Article 46-3-201, in order to obtain or retain a licence as a certification authority, a certification authority must:

(a) be either: (i) an attorney admitted to practice before the courts of this state, that attorney's partnership which engages principally in the practice of law if the attorney is a partner, or a professional corporation in which the attorney named in the license is a shareholder; (ii) a financial institution, a corporation authorized to conduct trust business, or an insurance company, if authorized to do business in this state; (iii) any title insurance or abstract company authorized to do business in this state; or (iv) the governor, a department or division of state government, other than the Digital Signature Agency, the attorney general, the Utah Judicial Council, a state court, a city, a county, or the Legislature provided that: (A) each of the governmental entities acts through designated officials authorized by ordinance, rule, or statute to perform certification authority functions; and (B) the state or one of the governmental entities is the subscriber of all certificates issued by the certification authority;
(b) be the subscriber of a certificate published in the repository provided by the division or in a recognized repository;
(c) qualify and hold an appointment as a notary public or employ at least one notary public;
(d) employ as operative personnel only persons who have not been convicted of a felony or a crime involving fraud, false statement, or deception;
(e) employ as operative personnel only persons who have demonstrated knowledge and proficiency in following the requirements of this chapter;
(f) file with the division a suitable guaranty, unless the certification authority is a governmental entity listed in Subsection (1)(a)(iv);
(g) have access to hardware and software suitable for fulfilling the requirements of this chapter according to division rules;
(h) maintain an office in Utah or have established a registered agent for service of process in Utah; and
(i) comply with all licensing requirements established by division rule.[26]

Accordingly, there are two other instruments that clearly lay down the conditions of establishment. One is the UNCITRAL Model Law on Electronic Signatures (Article 10), and the other is the China Electronic Signatures Law (Article 17).

From the author's perspective it is important that a certification authority should have sufficient financial resources so as to maintain its operations in conformity with its duties. Moreover, it is also essential that a CA should verify by appropriate means the identity and capacity to act of the person to

which a qualified certificate is issued. Finally, it is necessary that a CA should employ personnel that possess expert knowledge, experience and qualifications necessary for the offered services.

8.4 Contemporary issue: regulating online intermediaries – CAs

8.4.1 What are the duties of CAs?

The CA performs a role similar to a witness to a document and it is equivalent to those traditional professions such as notaries.[27] To promote the trust in identity and status of the parties involved in electronic transactions it is essential to define the rights and duties of CAs. According to the ABA's Draft Guidelines, to issue a certificate worthy of trust, the CA must: (1) have a valid and verifiable certificate of its own; (2) conduct the inquiry on which the certificate will be based; (3) accurately state facts in the certificate, including both the facts about the subject and the facts about the CA's investigation; and (4) maintain a certificate revocation list (CRL).[28] The CA's continuing duty to maintain the CRL in a form that can be rapidly and efficiently used by persons wishing to rely on a certificate is in itself significant evidence that the service element predominates in what the CA is selling.[29]

A CA's main duty is to provide certificates with accurate information about the CA and the subject of the certificate.[30] In order to increase confidence a certificate should, ideally, mention or refer to such elements as the identity of the CA, the facts upon which the identification of the subject of the certificate is based, the degree of investigation performed by the CA to confirm the facts stated by the subject of the certificate, the start and the dates of the certificate's validity and the location of the relevant CRL.

8.4.2 What are the contractual liabilities of CAs?

Liabilities in the world of electronic commerce are complicated and legislators have recognised the need to balance the interests of the various parties who might be involved, either directly or indirectly, in a particular transaction.[31] Certification authorities are dependent on the ability of their certificates to inspire trust in the reliability of the information contained. Trust may be gained first and foremost from innumerable secure and successful communications in which certificates of a certain CA have proved to be reliable and trustworthy.[32] As provided by the EC Directive on Electronic Signatures, certification-service-providers providing certification-services to the public are subject to national rules regarding liability.[33] In addition, Article 6 of the EC Directive on Electronic Signatures states that: 'As a minimum, Member States shall ensure that by issuing a certificate as a qualified certificate to the public or by guaranteeing such is a certificate to the public a certification-service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate:

(a) as regards the accuracy at the time of issuance of all information contained in the qualified certificate and as regards the fact that the certificate contains all the details prescribed for a qualified certificate;
(b) for assurance that at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate;
(c) for assurance that the signature-creation data and signature-verification data can be used in a complementary manner in cases where the certification-service-provider generates them both;

unless the certification-service-provider proves that he has not acted negligently.

Suppose that a CA is wilfully or grossly negligent, or a CA conspires with the subject of the certificate, then the CA should obviously be liable for its actions and omissions. On the other hand, beyond the scope of this preliminary exploration, there are some other ways, which are not as straightforward as we mentioned above. These include:

> (1) the certificate is accurate, but the transaction goes wrong for some other reason; (2) The security of A's Key is compromised and D uses it, along with A's publicly available certificate, to impersonate A; (3) A revokes her key because she learns of D's actions, but D manages to transact during the period between A's revocation notice to the CA and the CA's posting of a certificate revocation; (4) The security of a CA's key is compromised and D begins issuing bogus certificates or bogus certificate revocations; (5) a CA erroneously lists A's key as revoked, and B refuses to transact with A; and (6) The meltdown scenario: there is a major discovery that the number theory or computation and the algorithms on which A and CA's keys are based are no longer secure.[34]

However, the CA should be liable when it fails to take proper evidence of the holder's identity, when it fails to keep proper records of preventing forged certificates to be produced, and of revocations. It should also be liable for its dishonest staff to contain unreliable records in certificates. Although there are so many possibilities available, the most common liability may be caused by misrepresentation.

Liability for misrepresentation

A simple example of misrepresentation might occur if a CA has failed to notice somebody's (A's) misrepresentation, relating to his identity or credit rating, when issuing the certificate. If a third party B suffered any loss after having entered into a business relationship with A on the reliance of an

incorrect certificate then the CA might be held negligent for having failed to thoroughly investigate A before issuing the certificate, and liable to B under the law of obligations.[35] The question that needs to be answered is whether the CA may be responsible under contract or tort law.

Under contract law, B, who after having relied on an incorrect certificate is the victim of a financial loss, will only be able to sue the CA if he can prove a breach of contract.[36] However, contractual relations are only established between the CA and A and between A and B.[37] There is, thus, no contractual relationship between the CA and B. Being outside the contractual sphere, B will have to prove the CA's responsibility on a tortious basis.

The CA may be tortiously liable if it was under a duty of care to provide accurate statements. The scope of that duty of care may depend on the level of inquiry it promised to carry out before issuing A's certificate. Evidence of that duty of care might be found in the certification practice statement which a CA would incorporate into a certificate. If the CA, for example, indicated in its practice statement that it would thoroughly check identity before issuing a certificate it might be guilty of negligence if it failed to notice that it had been presented with an obvious forgery.[38]

According to Recital 40 of the EC Directive on Electronic Commerce service providers have a duty to act, under certain circumstances, with a view to preventing or stopping illegal activities.[39] Article 11 of the UNCITRAL Model Law on Electronic Signatures also provides that: 'a relying party shall bear the legal consequences of its failure' to take reasonable steps to verify the reliability of an electronic signature and the validity, suspension or revocation of the certificate, and to observe any limitation with respect to the certificate.[40] However, it might not always be that easy for a third party to prove the CA's negligence because of the complexities of the technical process involved. Hence, strict liability should be applicable. Although strict liability is usually applied in cases involving goods it might apply if a certificate, which used a faulty algorithm to produce the CA's digital signature, was found to have a design defect. In the author's view, the CA and not the relying party should bear the burden of proof in contractual or tortious liability cases,[41] because in the case of electronic transactions a CA might be in a better position to insure the risk connected with an unreliable certificate. Hence, it should be acknowledged that a CA should be strictly liable to any third party or the failure to detect A's misstatements and have duties to prove a breach of contract or negligence in the actions. This would, of course, impose a heavy burden on every CA to insure the veracity of every CA.

Limitations of liability when all parties act reasonably

It goes without saying that it is in the CAs' best interest to try and limit their liability. In order not to endanger the viability of the CAs' industry it is of paramount importance that a CA should not be liable if it acted reasonably. If a subscriber has suffered financial loss because of a fraudster he will be

inclined to attempt to sue the CA if the fraudster cannot be located or is insolvent. In the absence of legislation many CAs have defined and limited their levels of responsibility when issuing certificates in their own documentations. In the US the documents that define their standards of good practice and liabilities are Certificate Practice Statements (CPS), which are 'a statement of the practices that a CA employs in issuing certificates',[42] and the Relying Party Agreement (RPA), which 'notifies the relying party of the warranties, disclaimers, classes of certificates, liability limits and limitations of damages applying to an issued certificate'.[43] One, as yet unexplored, solution to avoid excessive responsibility would be for the insurance market to spread the risk and costs throughout the relevant players of the entire industry.[44]

The unpredictable nature of the CA's liability is due to the uncertainty and absence of regulation concerning its rights and duties. In an attempt to restrict the liability Article 6 of the EC Directive on Electronic Signatures states that the certification service provider shall not be liable for damage arising from the use of a qualified certificate which exceeds the limitations placed on the use of that certificate;[45] and shall not be liable for damage resulting from the maximum value of transactions for which the certificate can be used.[46] However, the legislation is lacking for CAs that go out of business. A CA ceasing business might have a disastrous effect on the certificate it issued in the past, and ultimately undermine its validity and, hence, its utility if for example the validity of a digital signature needed to be checked.[47]

8.4.3 What is the international regulatory standard of CAs?

The EU approach

The EU goes further than the US by offering a presumption of validity to specific technologies that create the electronic contract. The EC Directive on Electronic Signatures[48] follows a two-tier approach. Its first tier is to forbid discrimination between handwritten and electronic signatures and the second is to confer additional legal status to 'advanced' electronic signatures.[49] It sets the foundations for a secure environment, establishing a legal framework for the liability of CAs towards third parties. The concept of 'advanced electronic signature' is based on a qualified certificate and is created by a secure signature creation device. Furthermore, the Directive establishes two different liability regimes, which will apply depending on the kind of certificate. For qualified certificates liability of the issuing CA towards third parties has been harmonised by imposing minimum standards. All other certificates (i.e. non-qualified certificates) will continue to be governed by national general liability rules as they stand now.[50] At the same time the Directive recognises third countries' certificates as legally equivalent to certificates issued by CSPs in the EU, as long as there is a link with the EU or there is a bilateral or multilateral agreement between the EU and the third countries.[51]

As discussed above, the EU has provided high standards for CSPs. These standards, or legally equivalent ones, need to be implemented globally. For instance, if a US firm is engaged in a business transaction with an EU firm and is required to comply with EU law, the US firm should use an advanced e-signature instead of a basic one. It is further suggested that the advanced e-signature should be based on a qualified certificate created by a CSP, and all of the certification requirements in the US should be legally equivalent to those in the EU.[52]

The US approach

In the US the Uniform Electronic Transactions Act (UETA) is mainly concerned with general contract law that needs to adapt to new electronic or computerised technologies, e.g. concluding contracts via electronic agents or recognising electronic documents.[53] It establishes equivalence between manual and electronic signatures. In contrast to Article 2(1) of the EC Directive on Electronic Signatures the UETA focuses on verifying the intent of the signatory rather than on developing forms and guidelines.[54] Furthermore, the UETA created a legal framework for reliable and secure e-transactions and encourages in practice the private sector's self-regulatory policies, while, at the same time, it limits excessive governmental involvement in e-commerce as it has refrained from setting up any mandatory scheme regarding e-signatures and certificates. Moreover, the US definition of e-signatures is at the same time broader and more defined than its EU counterpart. The UETA has the same fundamental principle as the UNCITRAL Model Law on Electronic Commerce – that there should be no discrimination against data messages or electronic records, and that there should be parity of treatment between paper and electronic documents.[55]

Furthermore, the US Electronic Signatures in Global and National Commerce Act 2000 (ESIGN Act) has adopted a 'minimalist approach' or 'technology-neutral approach'. It states that a contract's validity cannot be denied simply because it is in electronic form and electronic signatures cannot be denied legal validity solely because they are not in written form.[56] It does not, in effect, require any minimum level of security for an electronic contract to receive the same basic legal enforceability as a written signature. However, the ESIGN Act has come under a lot of criticism from some legal scholars, arguing that it has in its present form serious flaws. Its pre-emption clause,[57] for instance, clearly indicates that it applies merely to business and commercial transactions in or affecting foreign or interstate commerce. Therefore, it creates an uncertain, vague, and unpredictable situation in which no one is entirely sure just what the applicable law is. It is suggested that the US Congress should set in place a national law applicable to all 50 states which would replace all existing state laws currently in effect.[58]

In addition, although the EU and US have greatly advanced the field of electronic signatures legislation, some limitations still appear in their

regulations. There is no provision clarifying who has the burden of proof of unlawful or insufficient authenticated certificates. This means that, for the time being, if a PC's system was defective, leading to an e-authorisation forgery or amendments to the context of an e-document, it will be the legitimate users' responsibility to prove that their PC's software collapsed or they were victims of fraudulent spending. As both the EU and US legislation do not limit the users' liability in these cases it is quite difficult for the user to prove the invalidity of a signature which is supported by a certificate issued by an accredited CA. Besides, for technical failure and abuse of an e-signature, users still carry the burden to provide evidence in disputes over e-transactions in case of human error. Therefore, as far as future harmonisation is concerned there is a lot of work to be done both on the governmental level and for the private sector. Further, results will definitely be achieved if the EU and the US continue their transnational dialogue and cooperate with other international bodies for the proliferation of a reliable and consistently standardised e-commerce.[59]

The Chinese approach

In China the China Electronic Signatures Law is formulated for 'the purpose of regulating the act of electronic signature, establishing the legal effect of electronic signature, and maintaining the lawful rights and interests of the relevant parties concerned'.[60] Some scholars argued that, like most countries that have enacted an e-signatures law, China takes a technology-neutral approach in how e-signatures are defined so as not to hinder technological evolution or to favour one technology over another.[61] In contrast other scholars argued that the China Electronic Signatures Law adopted a two-tier approach.[62] Under the first tier, without prejudice to any rules of evidence, an electronic signature or record shall not be denied admissibility in evidence in any legal proceedings on the sole ground that it is an electronic record.[63] At the second tier, if a rule of law requires the signature of a person or provides for certain consequences if a document is not signed by a person, a digital signature of the person satisfies the requirement, but only if the digital signature is qualified as a 'secure' digital signature.[64] In the author's opinion the China Electronic Signatures Law is vague and answers with no certainty whether it is a technology-neutral approach or a two-tier approach. However, it is necessary that China's legislation tends to a two-tier approach because the massive internet population and dispute cases need to adopt stricter and more specific rules to govern the e-commerce system. However, one of the merits of the Chinese Electronic Signatures Law is that it gives the same legal validity and effect to e-signature certificates issued by both domestic and overseas CSPs. This would facilitate cross-border online transactions.[65]

From the discussion above it is notable that the levels of regulation in the EU, US and China are different. The fundamental differences in policy orientations and legislative perspectives will hinder, rather than promote,

international electronic commerce. Legislators from different countries should participate more actively in dialogue and co-operation towards global regulatory harmony.[66]

International harmonisation

International harmonisation of the law of electronic signatures depends on the success of an internationally consistent standard of electronic signatures as well as the legal recognition of foreign certification and electronic signatures.

The rule of 'functional equivalents' employed in the validity of electronic signatures and authenticated certificates should be considered the key principle to facilitate the harmonisation of standard and cross-border recognition of foreign certificates and electronic signatures.

With regard to the recognised international standard of electronic signatures the UNICITRAL advanced a full Model Law on Electronic Signatures in accordance with Article 7 of the UNCITRAL Model Law on Electronic Commerce, intending to reflect a function-equivalent approach to traditional paper-based concepts.[67] The Model Law on Electronic Signatures adopts a two-level definition of electronic signatures, and extensively provides for a PKI system of digital signatures through a three party conceptualisation of the duties and responsibilities of parties in the context of electronic signatures.[68] This essentially sets the ground for any national or regional approach to electronic signatures.

With regard to the recognition of foreign certificates and electronic signatures, Article 12 of the Model Law on Electronic Signatures specifies that:

1. In determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had:
   (a) To the geographic location where the certificate is issued or the electronic signature created or used; or
   (b) To the geographic location of the place of business of the issuer or signatory.
2. A certificate issued outside [the enacting State] shall have the same legal effect in [the enacting State] as a certificate issued in [the enacting State] if it offers a substantially equivalent level of reliability.
3. An electronic signature created or used outside [the enacting State] shall have the same legal effect in [the enacting State] as an electronic signature created or used in [the enacting State] if it offers a substantially equivalent level of reliability.

Article 12 explicitly recognises foreign certificates and signatures without geographical discrimination. It is notable that 'substantially equivalent' is the main test of the level of reliability of foreign certificates and electronic signatures. It further provides the flexibility of the standard by introducing

the principle of party autonomy in Article 12(5) of the Model Law on Electronic Signatures. It expresses that where parties agree to the use of certain types of electronic signatures or certificates, that agreement shall be recognised as sufficient for the purposes of cross-border recognition, unless that agreement would not be valid or effective under applicable law.[69]

In essence the UNCITRAL Model Law on Electronic Signatures is not designed to bring equally binding uniform rules throughout the world; rather it helps to harmonise legal standards with sensible supranational concepts. At the same time it leaves enough leeway for states to add rules that are specific or desired for their legal system. Additionally, it facilitates further law reform on a global level. This law-making method, from international model laws to national legislation, 'may also pave the way for supranational methods to apply these new legal rules for electronic commerce in a uniform or harmonised manner despite the different legal traditions'.[70]

There is no doubt that international instruments, like the UNCITRAL Model Law on Electronic Commerce and the UN Convention on the Use of Electronic Communications, are important in encouraging transnational electronic commercial transactions and building trust through legal certainty. The international legislative instruments should take into account the lack of common international technical standards, the constant existence of security and fraud threats as well as the absence of a common legal base regarding cross-border transactions.[71] So as to further respond to the growing international electronic cross-border transactions the international harmonisation of legislation becomes even more significant. To facilitate international harmonisation, in particular, the legal recognition of foreign certificates and electronic signatures, the Working Group IV of the UNCITRAL requested the Secretariat to continue working on these issues.[72] The 2007 UNCITRAL Report on Promoting Confidence in Electronic Commerce, released in February 2009, complements the existing international instruments, further enhancing legal issues on international use of electronic authentication and signature methods.[73] International obstacles in promoting the use of electronic signatures in international commerce are created by conflicting technology-specific national approaches. It is observed that one of the main obstacles to the cross-border use of electronic signatures and authentication has been a lack of interoperability, due to conflicting or divergent standards or their inconsistent implementation.[74] Business and legal compatibility and technical interoperability of authentication schemes can be deployed at both national and international levels, to facilitate cross-border online interactions and transactions in both the private and public sectors.[75] UNCITRAL recommends building sophisticated mechanisms for recognising foreign authentication services and working on national rules on liability of certificate service providers complying with a uniform international standard. In the 2007 UNCITRAL Report on Promoting Confidence in Electronic Commerce, it is confirmed that the two principles – 'place of origin, reciprocity and local validation' and 'substantive equivalence' – originated

from Article 12 of the Model Law on Electronic Signatures should be employed by national laws to enhance the international standard of security and remove the obstacles to the recognition of foreign certificates and electronic signatures. It also points out that cross-recognition would typically occur at the PKI level rather than at the level of the individual certification services provider. The application of technical interoperability as well as the harmonisation of certificate policies and practice statements will contribute to the promotion of cross-certification and reorganisation.

After all, creating trust and building confidence in electronic commerce is of great importance for its development. Special rules in the recognition of foreign certificates and electronic signatures may be needed. International legal instruments, transnational model laws, national legislation, self-regulatory instruments or contractual agreements should be modernised and well developed to increase certainty and security in its use with special rules.[76]

9 Contemporary issue: protecting information in electronic communications

As discussed in previous chapters, encryption is used to determine identity and verify electronic signatures. Another area where encryption or digital signatures may give rise to practical problems is data security and privacy protection. For example in B2C transactions an online retailer might have a database of information about its customers' personal details and their history of transactions. In B2B transactions an international trading company might have its business partners' bank details and business strategies in their computer servers after issuing Electronic Bills of Lading and Electronic Letters of Credit. So what will happen:

a if a third party steals the information; or
b if the database owner sells the information to the third party?

Data security and privacy guarantees are vital in electronic commerce as it boosts users' confidence in making electronic commercial transactions. The United Nations Commission on International Trade Law (UNCITRAL) tried to enhance these two extended issues – data and privacy protection. In its recent report 'Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods', released in February 2009,[1] UNCITRAL addresses the privacy and confidentiality requirements of internet service providers in order to increase the legal certainty in protecting personally identifiable information as well as trade and competitive data.

In bygone days, spies could enter one's residence, organisation or company and collect valuable data information such as personal sensitive data, trade secrets or transaction records. Nowadays the open architecture of the internet has generated an environment in which it is much easier,[2] quicker and wider to collect data than it used to be because a variety of sensitive information can be captured on the internet without personal presence in the location where the data is situated.

There are several ways that internet users' information can be collected and stored:

a) Clickstream: a clickstream happens when an individual visitor clicks on a link on a website. The click information including visitors' IP addresses, visiting geographical location, type of browser software and other web activities will be captured by the server hosting the website. The information is usually collected for web activity analysis, market research and sales promotion; however, it might be used unfairly or unlawfully to sell or share users' clickstream data to a third party.

b) Computer Series Number and Software Product Key Code Registration: activation of a computer is a mandatory procedure when setting up a computer, while registration of software is usually required when installing computer programs. During this process, the service provider might ask you to provide personal information, i.e. address and email for the record of after sale service. For example, Microsoft has 'Windows Product Activation' tool, collecting the users' CPU serial number and CPU model number/type. During activation users may also provide personal information if users want to register their product with Microsoft.[3] During other software instalments users' registration may also be recommended. It entitles users to receive information about product updates and special offers directly from the service provider, i.e. Microsoft. Generally, service providers should make a privacy protection statement that all registration information provided is stored securely and no information is ever loaned or sold to third parties.

c) Cookies, Web bugs and Spyware: a 'cookie' is data or a text file that is sent to users' browser and stored on users' computer's hard drive to track users' personal information and visiting or usage patterns. The ostensible purpose of cookies is to facilitate customised services to the user, but the potential for misuse of such data is considerable and well documented.[4] In addition a cookie can be stolen via a network. In modern browsers users can be notified when a cookie is sent so as to accept or reject all cookies by setting preferences in the browser.

   Web bugs, a variation of cookies, are graphic images that are invisible to visitors. They can be embedded in emails and web pages. They can track the information on the dispatch of emails with the recipient's email address. Unlike cookies they cannot be prohibited by traditional internet browser settings.[5]

   Spyware is another method of information theft. It is software installed surreptitiously on personal computers without the knowledge of the subscriber or user. Such software cannot usually be uninstalled. It is used to gain access to information, store information or trace the activities of the user.[6]

d) Online Shopping: companies providing online shopping platforms, such as eBay, Amazon and Alibaba etc, have a large amount of online shoppers' sensitive personal information, including name, credit card details, delivery address, email address and product preferences. Such information is usually stored in the company's database server for a period of

time for the purposes of keeping purchase records, doing market analysis and researching product promotion. Although it is recommended that users should read the website's privacy and security policies before they order, it is unknown whether every company will strictly comply with their policy.

e) Social Networking or Online Dating Sites: social networking websites, such as Facebook, linkedIn and mySpace etc, contain a variety of personal information, including personal profile, contact information, social circle of friends, comments from and to friends, personal interests, photos, joined groups or professional information. Online dating sites, such as eHarmony and Match.com etc. publish your sensitive private information, i.e. age, sexual preferences etc. All the information might be at risk of being sold or shared with third parties for various purposes depending on the terms and conditions of users' agreement or privacy policies.

f) Governments, Banks or Other Organisations: there is usually a large profile of sensitive personal information stored in the databases of governments, banks and other private or public organisations. For example, the domain name registration database WHOIS contains every domain name registrants' details including domain name address, name, home or company address and telephone numbers, which are published publicly.[7] The BBC also reported that a 'horrifying' number of companies, government departments and other public bodies have breached data protection rules.[8] It will damage social trust and cause social chaos if government agents misuse or trade personal data.

It is obvious that the examples given above concern both data and privacy protection. But what are the differences between them? In the author's view data security is the fundamental measure for privacy protection. In other words, in order to protect privacy rights data security must be ensured. Personal data protection should protect the rights of the data ownership and balance the benefits between the protection of the data ownership and the permission of data free-flow, whilst privacy protection is to protect fundamental human rights.

9.1 Data protection policies and practices

9.1.1 EU

As stated in Article 8 of the Convention of Human Rights and Fundamental Freedoms 1950 (hereafter the Human Rights Convention) private life should be protected:

> (1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in

> accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[9]

Article 8 of the Human Rights Convention shows that the right to privacy is a fundamental human right, and Article 8(1) details that a person's correspondence should be respected and protected. Mr Rolv Ryssdal, President of the European Court of Human Rights, also noted that 'activities in the field of data protection are firmly rooted in fundamental rights and freedoms'.[10]

When doing business online there is no transaction that exists without the confidence of the people, so the law needs to provide safeguards for the information that the customer does not consent to being retained. In response to the protection of private life under the Human Rights Convention, as well as promoting harmonisation of European economic activities and laws of 27 Member States[11] governing the free flow of personal data, the EC Directive on Data Protection was adopted in 1995.[12] The relationship between the Convention and the Directive can be found in Recital 10 of the EC Directive on Data Protection:

> Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community.

The Directive is deemed to be comprehensive and it is one of the most significant accomplishments in data protection in the EU by standardising the level, as expressed in Article 1 that:

> (1) In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. (2) Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

This means that if it is not against data protection law, companies are entitled to free movement of data within the EU. It is argued that the freedom to transfer personal data within the EU without fear of discriminatory

restrictions on data flows is a huge boon to companies engaged in electronic commerce.[13]

The EC Directive on Data Protection defines 'personal data' as 'any information relating to an identified or identifiable natural person ("data subject"); and identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.[14]

However, the EC Directive on Data Protection does not define 'sensitive personal data', although Recitals (34) and (70) of the Directive mention the term 'sensitive' data. In the UK the Data Protection Act 1998 clarifies the scope of 'sensitive personal data', which means personal information relating to:

(a) the racial or ethnic origin of the data subject,
(b) his political opinions,
(c) his religious beliefs or other beliefs of a similar nature,
(d) whether he is a member of a trade union,
(e) his physical or mental health or condition,
(f) his sexual life,
(g) the commission or alleged commission by him of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.[15]

Compared to the EC Directive on Data Protection, the UK Data Protection Act is clearer and stricter on the definition and scope of data that involves sensitive information. Such clarification will be helpful for the implementation of the Act. In the UK a breach of the Data Protection Act will expose a data controller to enforcement action by the Information Commissioner. For example, the Commissioner may issue an Enforcement Notice, whereas the main weaknesses of the EC Directive on Data Protection are that 'it has unclear objectives and insufficient focus on detriment, risk and practical enforcement'.[16] There are no specific enforcement measures to be adopted by Member States in the EC Directive on Data Protection except for the general requirement of 'suitable measures' in Articles 15 and 24, but without detailed explanation.

Still, the European Commission investigated whether the UK complies with the EC Directive on Data Protection. In the UK case of *Durant v the Financial Services Authority (FSA)*,[17] the interpretation of 'personal data' in the UK Data Protection Act was narrowed by the English Court of Appeal. It was held that personal data only refers to information that affects one's personal or family life, business or professional capacity. In response to the EC investigation, the Information Commissioner has published a discussion of the implications of the *Durant* case.[18] The Information Commissioner

confirms the court judgments on the measure of the scope of individual information that the individual information in question should be capable of having an adverse impact on the individual's privacy. The two notions of identification are recognised as a biographical sense and an individual focus as the judge ruled that:

> The first is whether the information is biographical in a significant sense, that is, going beyond the recording of [the individual's] involvement in a matter or an event which has no personal connotations; . . . The second concerns focus. The information should have the [individual] as its focus rather than some other person with whom he may have been involved or some transaction or event in which he may have figured or have had an interest . . .[19]

The commissioners deemed that the judgment provided helpful guidance and greater clarity regarding the complex meaning of 'personal data' and 'relevant filing system'.[20]

With regard to principles relating to data quality there are five principles laid down by Article 6 of the EC Directive on Data Protection specifying that personal data must be:

1) processed fairly and lawfully;
2) collected for specified, explicit and legitimate purposes;
3) adequate, relevant and not excessive;
4) accurate and up-to-date;
5) keep data subjects permitted for identification for a necessary period only.

Among these five principles the first principle is fundamental. The Directive further explained the first principle – how to process personal data legitimately – in Article 7 that data should be collected with the party's consent prior to entering into a contract.[21]

In the author's opinion the EC Directive on Data Protection is of great value in ensuring the level of harmonisation between Member States. It is a capacious directive that keeps in line with the ever-changing information technology to a large extent, although the Directive was adopted in 1995. However, in the EC Directive on Data Protection, there is only one provision dealing with the 'automated processing of data' – Article 15. There is a need to have complementary legislation particularising protection of online privacy and data security.

9.1.2 US

As stated in the EC Directive on Data Protection, personal data transfer to non-European Union nations that do not meet the European 'adequacy' level for protection will be prohibited. As a result, the EC Directive on Data

Protection may significantly hamper the ability of US companies to engage in many cross-border transactions, as there is no specific federal data protection legislation in the US. In order to bridge the gap and provide a streamlined means for US organisations to comply with the EC Directive on Data Protection the US Department of Commerce, in consultation with the European Commission, developed a 'safe harbour' framework approved by the EU in 2000.[22] The Safe Harbour Agreement is deemed to be 'an important way for U.S. companies to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by European authorities'.[23] The Safe Harbour Agreement encourages the development of international electronic commercial transactions between the EU and the US, as it not only promotes the transnational free flow of data information but also protects cross-border privacy rights. The practices and benefits of the Safe Harbour Agreement to privacy rights will be discussed in the next section – Internet Privacy. The safe harbour privacy principles are: notice, choice, onward transfer, security, data integrity, access and enforcement.

9.1.3 China

China, similarly to the US, currently has no national data protection law. However, there are national legislative measures to address data security concerns. For example, the Ministry of Public Security of the People's Republic of China promulgated the Measures for Security Protection Administration of the International Networking of Computer Information Networks[24] in 1997. The Regulation of the People's Republic of China for Security Protection of Computer Information System was promulgated by Decree No. 147 of the State Council of the People's Republic of China[25] in 1994.

During 2008 and 2009 several provinces and cities across China also introduced independent local legislative measures. For example, in April 2009, the Standing Committee of the People's Congress in Hangzhou City of Zhejiang Province announced the Measures for Computer Information Network Security Protection Administration.[26] The Regulation of the Guangdong Provision for Security Protection of Computer Information System was also effective in April 2008.[27]

The national and local measures and regulations play a significant role in protecting data security in China; however, a single integrated national law is still needed to 1) promote a secured environment for international data flows; 2) harmonise different national and local rules so as to provide legal certainty at the national level; 3) promote confidence in data security and personal privacy in both offline and online situations. In response to the protection urge of personal information, the PRC State Council commissioned the legal research institute of the Chinese Academy of Social Sciences to draft the Law for Personal Data Protection of the People's Republic of China. The draft was published in 2005 and provided rules protecting personal information, data and privacy.[28] In the author's opinion, because China is a civil law

country implementing written laws, its legislative methodology is much more similar to some continental European countries than the US. The structure and model of PRC Personal Data Protection Law should be learned from the European legislative approach, although it should also be influenced by parts of the advanced US legislative agenda. In order to meet the international standard of data protection China should draw its national data protection rules in compliance with the Guidelines of the OECD and APEC, although the condition and culture of the state should be considered. If the future PRC national data protection law has some significant differences from the third country, China can advise on international negotiation and reach bilateral or multilateral agreements learning from the experience of the EU–US Safe Harbour Agreement.

9.2 Internet privacy: regulations and practices

Privacy, as a fundamental human right, has been protected under basic laws in different countries or conventions at the international level since the 1950s. From a boom of electronic commercial transactions in 2000, data protection stemming from international computer networks has been challenged due to technical and legislative obstacles. Data protection constraints on the internet are preventing the full protection of online users' privacy rights. In order to build web users' confidence, online trading or service companies have posted self-regulations on webpages. However, it is impossible to know how many users have actually read the privacy statement in small print or via a clicked link before using the service or placing the order. The question is also raised as to whether companies do keep their promises and comply with the self-regulated privacy policies. If not, what are the remedies?

In response to the necessity of e-privacy legislation, countries, in particular developing countries such as European countries and the US, have made efforts to regulate the rules of e-privacy. International organisations such as APEC have also undertaken the responsibility to harmonise an e-privacy international protection standard in order to facilitate economic growth, co-operation, trade and investment in the Asia-Pacific region.[29]

9.2.1 International framework

As mentioned earlier, back in the 1980s the Organization for Economic Co-operation and Development (OECD) pioneered the international guidelines on privacy protection. The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were promulgated in Paris in 1980 (hereafter OECD Guidelines),[30] which apply to 30 OECD countries, including the UK, the US, some other European countries, but not China.

There are eight basic principles of privacy protection in the OECD Guidelines:

1) Collection Limitation Principle;
2) Data Quality Principle;
3) Purpose Specification Principle;
4) Use Limitation Principle;
5) Security Safeguards Principle;
6) Openness Principle;
7) Individual Participation Principle;
8) Accountability.

The eight principles have influenced national and community legislation. For example, the EC Directive on Data Protection in 1995 has adopted the first five principles of data protection in the OECD Guidelines. There is no doubt that the OECD Guidelines have taken the lead in harmonising national privacy legislation and their significant role cannot be ignored. However, the OECD Guidelines were drafted almost 20 years before the spread of information technology; thus, its working group started to examine whether the OECD Guidelines are still suitable for the modern information society in the late 1990s and reported its opinion in 'Implementing the OECD "Privacy Guidelines" in Electronic Environment: Focus on the Internet' (hereafter OECD Export Report) in 1998.[31] The OECD Export Report reaffirms that the Guidelines are applicable with regard to any technology used for collecting and processing data and there is no need to revise the OECD Guidelines, although a dialogue between the private sector and individual users of networks will be useful in order to learn about business needs and consider technical solutions.

In the author's opinion the features of online commercial transactions are unique when compared with those of offline transactions. Cross-border transfer of data is much easier, faster and wider in the online world. The basic principles of privacy protection in the OECD Guidelines should still be sufficient to protect online data stored in computer hard drives – which are similar to data traditionally stored in safe cupboards. However, the principles must be reconsidered to protect online data that has been captured in transit via the internet or sold commercially by electronic means. The trans-border flow of data will naturally raise the volume of cross-border privacy disputes. It challenges the enforcement of transnational cases. Thus, in the author's view, two extra principles – 'transparency' and 'enforceability' – should be considered as additions to the OECD Guidelines. This view is justified by the OECD 'Report on the Cross-border Enforcement of Privacy Laws' in 2006 which states that 'greater transparency about how privacy enforcement works would be helpful for business compliance and user trust in global privacy protection'.[32]

In response to the need for an up-to-date international framework on privacy protection, APEC endorsed the APEC Privacy Framework in 2004, developed by its Electronic Commerce Steering Co-operation. It is based on the core values of the OECD Guidelines. There are 21 APEC member

economies including China, US, Australia and Canada.[33] As mentioned earlier the US, Australia and Canada are OECD members, but not China. So the OECD Guidelines and APEC Privacy Framework together should cover the key economic layers in the world. The APEC Privacy Framework was developed in recognition of the importance of developing appropriate privacy protections for personal information, removing barriers to information flows and enabling enforcement agencies to fulfil their mandate to protect information.[34] In other words its aim is to balance private rights and information flow and to enhance enforcement of privacy protection. It reflects on the 8 principles of the APEC Privacy Framework as below:

1) Preventing Harm
2) Integrity of Personal Information
3) Notice
4) Security Safeguards
5) Access and Correction
6) Uses of Personal Information
7) Accountability
8) Choice.

Compared with the OECD privacy principles, there are two different principles in the APEC Privacy Framework, which are: 'preventing harm' and 'choice'. These two principles show APEC's efforts to facilitate responsible information flows in order to encourage the growth of e-commerce rather than only to protect human rights. The issue of building enforcement agencies and mechanisms has not been listed as one of the separate principles but it has been discussed within the first principle – 'preventing harm' and other provisions.

The OECD Guidelines and APEC Framework serve as references for national legislation voluntarily but not mandatorily. At the international level, there is no single legislation on privacy issues at the United Nations Commission on International Trade Law (UNCITRAL), thus UNCITRAL continues to give further explanation as to its existing electronic commerce convention and model laws relating to privacy issues. It published an official note on 'Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods'[35] in 2009. This note has taken a number of references from the OECD Guidelines and APEC Privacy Framework which intends to provide legal consistency and certainty of privacy protection. It identifies the difficulties in relation to privacy protection in identity management systems,[36] therefore it proposes the issuance of 'citizen cards' by public authorities – an official document for electronic administrative procedures including commercial transactions to preclude data-sharing issues and protect data privacy.[37] In the author's opinion such an identity infrastructure is of a higher level than the Trustmark or Seal scheme; however, time and cost may be the two most significant barriers

to issuing citizen cards at the first stage. At the second stage, technology support might be different in different countries, which might become another obstacle to the promotion of cross-border information flow.

9.2.2 EU

As discussed earlier the EC Directive on Data Protection 1995 protects not only personal data but also individual privacy rights.[38] It reflects on Recital 6, 12 and Article 1 of the EC ePrivacy Directive. For example, Recital 6 of the EC ePrivacy Directive states that 'the Internet is overturning traditional market structures by providing a common, global infrastructure for the delivery of a wide range of electronic communications services. Publicly available electronic communications services over the Internet open new possibilities for users but also new risks for their personal data and privacy'. Recital 12 further clarifies that by supplementing the EC Directive on Data Protection, the EC ePrivacy Directive 'is aimed at protecting the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons'. Moreover, Article 1 of the EC ePrivacy Directive provides that:

1) This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.
2) The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.

Although the EC ePrivacy Directive complements the EC Directive on Data Protection providing privacy protection particularly in the electronic communication sector, some provisions of the EC ePrivacy Directive are narrow or non-specific. For example, Article 4 Security and Article 6 Traffic Data need to be amended for regulating the liability of data infringement. On 13 November 2007 the European Commission adopted a Proposal for amending the EC ePrivacy Directive. In response to the proposal the European Data Protection Supervisor (EDPS) released his second Opinion on ePrivacy Directive review and security breach in January 2009.[39] The EDPS welcomes the adoption of a security breach notification system as it will encourage companies to improve data security and enhance the accountability of the personal data.[40] That is, network operators and ISPs should notify security breaches to the National Regulatory Authorities (NRAs) and

also their customers. However, it is argued that the Communication is unclear in terms of its scope of the organisation that is subject to breach notification as it seems to only refer to IT companies in the EU, whereas most state legislation in the US applies 'horizontally to all organisations that process certain types of information'.[41]

The substantial issue of the liability of infringement of privacy rights shall be governed by national laws. As stated in Recital 55 and Article 23 of the EC Directive on Data Protection any person who has suffered damage is entitled to receive compensation from the controller, as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive. Article 15(2) of the EC ePrivacy Directive also provides that the provisions of judicial remedies, liability and sanctions of the EC Directive on Data Protection shall apply with regard to national provisions adopted pursuant to this Directive. An example can be given by a leading case in the UK that hit the headlines in 2008 – in *Applause Store Productions Ltd and Firsht v Grant Raphael*[42] (hereafter Facebook case) the claimant Mathew Firsht, the owner of Applause Store Productions, was successful in an action alleging libel and misuse of private information. It was a lawsuit against the claimant's former friend, Grant Raphael, who created a false profile for Mathew Firsht on Facebook without his consent. The defendant published the claimant's sensitive personal information on Facebook and created a link called 'Has Mathew Firsht lied to you?' which defamed Mathew's business in providing audiences for popular television programmes. The Judge Richard Parkes QC ruled that the claimant, Mathew Firsht, be awarded £2,000 for damages compensation of his hurt feelings and distress caused by the defendant's misuse of private information, along with other compensation for damages of defamation.

9.2.3 US

While the EU has comprehensive legislation on data privacy protection the US has a different approach, known as a market-dominated or market-based approach as there is no comprehensive federal legislation towards the protection of privacy rights. Although there is an Electronic Communications Privacy Act (ECPA), it was adopted for the telecommunication industry in 1986 before the boom of e-commerce. Since 1995 the Federal Trade Commission (FTC) has made efforts in recommending online privacy protection.[43] Thereafter the FTC has surveyed online information practices and published three reports. The most recent report by the FTC was published in May 2000, entitled 'Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress' (hereafter FTC Fair Information Practices Report).[44] It was an amalgamation, amendment or improvement of the first two reports: 'Self-Regulation and Privacy Online: A Federal Trade Commission Report to Congress'[45] in July 1999 and 'Privacy Online: A Report to Congress'[46] in June 1998.

The FTC Fair Information Practices outlines five principles of privacy protection. They are:

1) Notice/Awareness
2) Choice/Consent
3) Access/Participation
4) Integrity/Security
5) Enforcement/Redress.

The FTC principles are identical to those in the EC Directive on Data Protection, OECD Guidelines and APEC Privacy Framework. However, the FTC report has the unique fifth principle – 'enforcement' – which hasn't been listed as a single separate principle in other national and international privacy policies. Enforcement, as identified by the FTC, is to use 'a reliable mechanism to impose sanctions for noncompliance with these fair information practices' in any governmental or self-regulatory program to ensure privacy online.[47] In the self-regulatory industry the privacy seal programs are considered to be one of the key enforcement mechanisms to emerge, whilst in the public section, the Commission has the authority to seek injunctive and other equitable relief or pursue remedies for deceptive information practices that infringe the relevant legislation such as the Children's Online Privacy Protection Act (COPPA). However, as there is no federal uniform privacy legislation in the US the FTC Commission will have no authority to require companies to adopt information practice policies or to abide by the fair information practice principles on their websites.[48] Most of the big companies, such as Amazon, Microsoft, Google and Facebook, have participated in the EU–US Safe Harbour Agreement and published their privacy policies on their websites. However, it is very hard to guarantee that companies will strictly comply with their self-regulated privacy policies. In recent years some of the big internet players have tried to merge in order to strengthen their market power, i.e. Google with DoubleClick; Microsoft with aQuantive; Facebook with Beacon; and eBay with Beacon.

On 21 December 2007, the FTC approved the Google and DoubleClick Merger without conditions. It raised privacy concerns for Google and DoubleClick's internet behaviour tracking and the European Commission have investigated the merger. The US Electronic Privacy Information Center (EPIC), a public interest research centre in Washington, DC, also filed a complaint about the merger case. The FTC's opinion remained the same. On 14 March 2008 EPIC sued the FTC to compel disclosure of documents concerning Jones Day's role in the US DoubleClick merger review.[49]

In 2007 the partnership of the social networking website Facebook.com and Beacon also raised privacy concerns in public as Facebook users who shop at third party websites will have their purchases notified to their friends via Facebook. In November 2007 the interest group MoveOn.org has started a petition campaign and Facebook group against this feature: Facebook were

under public pressure. On 4 December 2007 Facebook announced that users would be able to opt out of the Beacon advertising system. Facebook ensured that the opt-out boxes would be available on the website.[50]

Social networking sites have become popular with younger generations as a platform for socialising with friends and even facilitating companies' commercial transactions. In January 2009 EPIC suggested the regulation of social network service advertisers and application developers. It is debated whether the US–EU Safe Harbour Agreement clearly covers legal requirements of data privacy protection on social networking sites which are fast-growing after the adoption of the safe harbour agreement. The European Advisory Group – a working party set up under Article 29 of Directive 95/46/EC (EC Directive on Data Protection) – feels the need for regulation of social networking sites (SNS) to ensure compliance with EU law. It issued an opinion on social networking called 'Opinion 5/2009 on online social networking', adopted on 12 June 2009, providing guidance to social network service providers.[51] The working group is intended to provide key recommendations on the obligations of SNS providers and to uphold and strengthen the rights of users for the dissemination and use of information available on SNS for other secondary, unintended purposes. This opinion can serve as a particularised standardisation on the EU–US data protection agreement referring to social networking security issues.

9.2.4 China

Although the China Internet Network Information Center (CNNIC) suggested that 'the size of netizens in China surpassed that of the United States in June 2008 and ranked the first in the world' in the 23rd Statistical Report on the Internet Development in China in January 2009,[52] the Chinese legislation has not kept up to date with the development of the internet networking environment. Currently there is no specific e-privacy legislation in China. However, general privacy rights have been regulated under the Constitution of the People's Republic of China and the General Principles of the Civil Law of the People's Republic of China since the 1980s.

Article 38 of the Constitution protects the basic rights of personal dignity. It states 'the personal dignity of citizens of the People's Republic of China is inviolable. Insult, libel, false accusation or false incrimination directed against citizens by any means is prohibited', whilst Article 40 of the Constitution provides some significant restrictions to such rights in that 'Freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law. No organisation or individual may, on any ground, infringe upon citizens freedom and privacy of correspondence, except in cases where, to meet the needs of state security or of criminal investigation, public security is permitted to censor correspondence in accordance with procedures prescribed by law'.[53]

There is no clause governing privacy rights in China Civil Law, however

the General Principles of the Civil Law of the People's Republic of China specifies, in Article 101, that citizens and legal persons shall enjoy the right of reputation. The personality of citizens shall be protected by law, and the use of insults, libel or other means to damage the reputation of citizens or legal persons shall be prohibited.[54]

As stated above in the PRC Constitution and Civil laws, rules relating to privacy protection are indirect, simple and non-specific. Companies running businesses online should be encouraged to self-regulate on the privacy policy. The e-privacy policy should include the duties and liabilities of ISPs, the function and usage of cookies, the rights of control and access of personal information, the guarantee of data security, conditions of third party advertising and the protection of children's safety.[55] For example, one of China's largest and most used internet service portals, QQ (Tencent, Inc. founded in 1998), whose instant messaging platform has already profoundly influenced the way tens of millions of internet users communicate with one another, has its self-regulation on privacy protection on the website – 'Privacy Statement' updated on 24 April 2007.[56] This privacy statement regulates 11 issues: 1) Collection of Your Personal Information; 2) Control of Your Personal Information; 3) Security of Your information; 4) Use of Cookies; 5) Use of Web Beacons; 6) Use of Information within the Tencent Network; 7) Use of Information outside the Tencent Network; 8) Use of Third Party Ad Networks; 9) Access to Your Personal Information; 10) Collection and Use of Children's Personal Information; and 11) Exemption of Liability.[57] This statement is to ensure that the users' personal information will be used correctly and fairly. QQ/Tencent will notify the users when they collect their personal information and store such information in a secured system. In addition, all the collected information will be not shared with a third party unless pre-agreed. It is similar to the standard of data privacy protection in the EU–US Safe Harbour Agreement,[58] except for the principle of enforcement. There is no enforcement clause in QQ/Tencent's privacy statement and no technology specification of the data security protection system. Moreover, Tencent allows other companies, called third-party ad servers or ad networks, to display advertisements on Tencent webpages and place a persistent cookie on the users' computers. Tencent also exempts its liability from any dispute resulting from the use of personal information by any third party listed in the statement. All users who use QQ and Tencent instant messaging or web service are presumed to have read the privacy statement and agreed with the terms and conditions. The problem is that whether the users are aware of the privacy statement, and even if so, whether they will read it carefully before they decide to subscribe to any of the QQ/Tencent products, and whether they will keep paying attention to any changes in the privacy statement as 'Tencent will occasionally update this privacy statement'. Any update of the privacy statement will not necessarily be informed to the users as there is no duty of notification of amendment of the privacy policy.

The second distinguishing example of the development of China's online

privacy policy can be given by Alibaba.com, founded in 1999 – one of the world's largest online B2B marketplaces providing a trading platform for global small and medium manufacturers.[59] The privacy policy of Alibaba.com (global trade platform) was updated and published on 1 January 2009, whilst the privacy statement of Alibaba.com.cn (Chinese domestic trade platform) remained unchanged from 1999. Alibaba.com.cn clarifies that when the users agree to the Service Agreement, the users agree to the privacy statement as it is part of the Service Agreement.[60] The statement lists the provisions of (a) the protection of children; (b) usage of username and password; (c) usage of users' registration information; i.e. name, address, nationality, phone number and email address; (d) usage of cookies; (e) conditions of transferring information to the third party; and (f) security technology. The statement points out that one of the purposes of the collection of registration information is for statistical analysis for trade and service promotion. Alibaba.com.cn will record users' IP addresses for 60 days only for safety and national regulatory reasons if nothing concerning security is found. The company will not sell, rent, share and exchange users' personal information unless the third party affiliates or forms a partnership with Alibaba to support the operation of the site and services. The relevant measures of security will be complied with so that the personal information will not be stolen, misused and changed.

Although Alibaba.com and Alibaba.com.cn are the same organisation, they promote business in different jurisdictions. Alibaba.com targets the global market, while the latter specialises in Chinese demotic trade. It is an interesting finding that, within the same organisation, different branches promoting sale and production in different jurisdictions have separate or different privacy policies. The privacy policy of Alibaba.com is newer than Alibaba.com.cn. They are similar; however, compared with Alibaba.com.cn, Alibaba.com has more advanced clauses regarding collected information (including not only registration information and statistical information in Alibaba.com.cn but also publishing information and payment information); transfer of collected information to third parties; and amendment of privacy policy. Alibaba.com specifies that collected information will not be disclosed to third parties unless the users respond to the marketing, promotion or advertising message. Collected information may be transferred, stored, used and processed outside your home jurisdiction. In case of a merger with or transfer of business to another business entity, the company will transfer collected information to the entity. Any changes of policy will be posted on the website. If users do not agree to the new changes in the Privacy Policy, they should contact Alibaba.com in writing.[61] Again the duty of notification of changes of policy is not required.

The Alibaba privacy policies also raise concern as to why the privacy protection standard of Alibaba's Chinese domestic website is lower and less specific than that of Alibaba's global market website. Should the branches of companies comply with the headquarters' privacy standard although domestic law should be taken into account?

Possible solutions: From an overall international perspective

The main privacy principles in the OECD, APEC, EC Directive on Data Protection, EU–US Safe Harbour Agreement and FTC are 'notification', 'choice', 'security', 'data integrity' and 'accessibility'. Most of them also have the principle of 'accountability'. However, only the FTC and Safe Harbour Agreement include the principle of 'enforceability'.

Privacy policies are generally enforced either by national enforcement authorities, alternative dispute resolutions or court litigation. Those national enforcement authorities can impose sanctions or fines for privacy breaches. In the UK the enforcement authority is the Information Commissioner, whereas in the US the enforcement authority is the Federal Trade Commissioner. Self-enforcement is also encouraged as both the OECD 'Privacy Online: Policy and Practice Guidance'[62] in 2003 and FTC Fair Information Practices Report in 2000 found that fostering the adoption of self-regulatory enforcement mechanisms or initiatives, such as trustmark/seal programs, is beneficial in promoting effective global solutions with regard to privacy compliance. As stated in the FTC Fair Information Practices Report, 'industry's primary self-regulatory enforcement initiative has been the development of online privacy seal programs'.

A trustmark, known as a 'seal', is usually accredited by a trusted third party and displayed on the authorised website. It is designed to build users' trust in using the websites. It gives users certainty about the privacy policy standard on what kind of information a site gathers, what the site operator does with that information, and with whom that information is shared.[63] The well-known seal/trustmarks programs are TRUSTe, BBBOnline and VeriSign. Some companies' websites have been licensed by the online privacy seal program. For example eBay and Microsoft are licensed by TRUSTe, Alibaba.com is accredited by VeriSign etc. However, privacy seal programs are not widely supported by international and national legislation and only a relatively small percentage of sites have introduced online-privacy seal programs.

Both TRUSTe and BBBOnline have enforcement procedures: users can file a complaint and seal program providers can respond by imposing sanctions on accredited websites. Such sanctions may include:

1) requiring the Licensee to correct or modify personally identifiable information or change user preferences;
2) requiring the Licensee to change its privacy statement or privacy practices; and/or
3) requiring the Licensee to submit to a third-party audit of its practices to ensure the validity of its privacy statement and to ensure that it has implemented the corrective action required.[64]

However, seal program providers cannot require a Licensee to pay monetary

damages or take further steps to exempt them from legal violation. The complaint report will be published except for pre-agreement on confidentiality.[65] TRUSTe and BBBOnline are the sole judges of the dispute.

Mann and Winn recognised the kind of complaint forum provided by TRUSTe and BBBOnline as an alternative dispute resolution (ADR) mechanism.[66] In the author's view, TRUSTe Watchdog Dispute Resolution Forum and BBBOnline Complaint Forum are not arbitration, mediation or negotiation as they are much lower than the standard of ADR procedures. It raises some concerns as to why TRUSTe and BBBOnline do not offer normal online dispute resolution (ODR) procedures using a standard ODR platform, where a complainant can file a case and choose a neutral person such as an assisted negotiator, mediator or arbitrator to help resolve the case. TRUSTe and BBBOnline might save costs and avoid complication in the sole judgment, but it might be fairer, more trustworthy or reliable and professional to adopt an efficient ODR procedure as cases involving privacy breaches are usually not very simple. They require expert investigation.

Seal programs' ODR service can be provided by any of two means. The first method would be that seal program service providers could purchase or produce user-friendly ODR software and appoint qualified assisted negotiators, mediators and arbitrators. The second method would be that seal program service providers could form partnerships with independent ODR service providers and publish the agreement that seal accredited privacy-policy disputes would be resolved by their ODR partner. It is worth noting that, as mentioned earlier, eBay is accredited by the TRUSTe seal program, while eBay users' disputes are compulsorily resolved by SquareTrade (an ODR service provider) before they go for litigation. In other words, eBay users have different channels to resolve different types of disputes: privacy-related issues on TRUSTe Watchdog Dispute Resolution Forum and business-related issues on SquareTrade. In these circumstances it might make sense that SquareTrade is also designated to resolve eBay users' TRUSTe privacy-policy disputes to enhance the users' confidence in providing personal information to proceed with commercial transactions.

Summary

Electronic signatures and authentication, as a means of providing safety and reliability in e-transactions, play an important role in e-commerce as it creates trust and confidence. With the rapid uptake of electronic commerce, predictably, there has been a rush to enact laws. These laws may suffer from two fundamental problems: the changing nature of the technology has the potential to render any legislation redundant within a short period of time. In addition, national laws are inadequate to govern what is truly a global issue. Regulation poses further threats in that it risks stifling electronic commerce if it is unduly burdensome.[67] Trust and security are now, more than ever, critical issues in doing business, whether online or in the paper world.

The development of global legislation in relation to data protection, information security, electronic signatures, and the control of encryption technology has become vital to facilitate international commerce.

One way to achieve legal certainty and predictability is through harmonisation. International, regional and national laws attempt to reduce legal barriers by using electronic technology to sign contracts. However, the liabilities and remedies of certification authorities are not substantially addressed in particularised e-commerce laws while CAs, as trusted third parties, are significant in identifying or authenticating persons who are not previously acquainted but wish to transact with one another over the internet. The more general lack of international regulatory and legal standardisation on establishing requirements and liabilities of CAs may prove to be a large obstacle to the development of reliable electronic commerce. Therefore, it is necessary to monitor international uniform regulations, and harmonise and implement international standard rules for the recognition of foreign electronic signatures and authentication.

Data privacy protection also relies on secure and reliable electronic signatures and authentication. Currently the international, EU and US privacy legislation or guidelines have their different preferences. The EU legislation is aimed at protecting individual privacy rights, whilst the US and international guidelines target promotion of the free flow of cross-border data for the development of global economy. There is one aspect in common: they all make efforts to balance individuals' privacy rights and entrepreneurs' marketing rights at the level of international harmonisation. The trustmark program, provided by a trusted third party certifying the quality of merchants' data privacy, should be deemed to be one of the most effective approaches in enhancing users' trust and confidence in online interactions.