Law of Electronic Commercial Transactions

Contemporary issues in the EU, US and China

Faye Fangfei Wang

Routledge Research in IT and E-Commerce Law

Law of Electronic Commercial Transactions

The exponential growth of electronic usage in global commercial transactions has generated potential opportunities in productivity, facilitated the cross-border free movement of goods and services, and stimulated export and import trade as well as domestic sales, but at the same time it has led to new challenges to existing laws due to the unique characteristics and complexities of online technology, culture and social behaviours.

This book compares the legislative frameworks of e-commerce in the EU, US, China and International Organisations. It highlights and analyses the main legal obstacles to the establishment of trust and confidence in doing business online. It provides in-depth research into finding solutions to remove the barriers to the validity of electronic contracts and signatures, the enforceability of data privacy protection, the determination of internet jurisdiction and choice of law, as well as the promotion of online dispute resolution. It encourages modernisation and harmonisation of laws concerning electronic commercial transactions through well-balanced area-specific international instruments.

Law of Electronic Commercial Transactions will be of great interest to academics, legislative organisations, practitioners and lawyers in the field of international commerce.

Dr Faye Fangfei Wang is a Senior Lecturer in Law at Bournemouth University, UK. She holds a PhD from the University of Southampton, an LLM from the University of Aberdeen, and an LLB from China. She specialises in cyberlaw, international trade law, conflicts of law and online dispute resolution.

Routledge Research in IT and E-Commerce Law

Forthcoming titles in this series include:

The Current State of Domain Name Regulation: Domain Names as Second Class Citizens in a Mark-dominated World
Konstantinos Komaitis

Online Dispute Resolution for Consumers in the European Union
Pablo Cortés

Law of Electronic Commercial Transactions

Contemporary issues in the EU, US and China

Faye Fangfei Wang

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First published 2010
by Routledge
2 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

Simultaneously published in the USA and Canada
by Routledge
270 Madison Avenue, New York, NY 10016

Routledge is an imprint of the Taylor & Francis Group,
an informa business

This edition published in the Taylor & Francis e-Library, 2010.

To purchase your own copy of this or any of Taylor & Francis or Routledge's
collection of thousands of eBooks please go to www.eBookstore.tandf.co.uk.

British Library Cataloguing in Publication Data
A catalogue record for this book is available
from the British Library

Library of Congress Cataloging in Publication Data
Wang, Faye Fangfei.
Law of electronic commercial transactions : contemporary issues in the
EU, US, and China / Faye Fangfei Wang.
p. cm.
Simultaneously published in the USA and Canada.
1. Electronic commerce—Law and legislation. 2. Contracts—
Automation. 3. Data encryption (Computer science)—Law and
legislation. 4. Internet domain names—Law and legislation. I. Title.
K1005.W35 2010
343.09′944—dc22 2009030558

ISBN 0-203-86000-4 Master e-book ISBN

ISBN10: 0–415–55745–3 (hbk)
ISBN13: 978–0–415–55745–0 (hbk)

ISBN10: 0–203–86000–4 (ebk)
ISBN13: 978–0–203–86000–7 (ebk)

Contents

Table of cases

Abbreviations

AAA	American Arbitration Association
ABA	American Bar Association
ADNDRC	Asian Domain Name Dispute Resolution Centre
ADR	alternative dispute resolution
APEC	Asia Pacific Economic Cooperation
B2B	business-to-business
B2C	business-to-consumer
CAs	certification authorities
CIETAC	China International Economic and Trade Arbitration Commission
CISG	United Nations Convention on Contracts for the International Sale of Goods
CLC	Contract Law of China
CMI	Committee Maritime International
CNDRP	CNNIC Domain Name Dispute Resolution Policy
CNNIC	China Internet Network Information Center
COPPA	Children's Online Privacy Protection Act
CRL	Certification Revocation List
CSPs	certification service providers
EC	European Commission
ECPA	Electronic Communications Privacy Act
EDPS	European Data Protection Supervisor
EPIC	Electronic Privacy Information Center (US)
ESIGN Act	Electronic Signatures in Global and National Commerce Act
EU	European Union
FTC	Federal Trade Commission
GUIDEC	General Usage for International Digitally Ensured Commerce
HKIAC	Hong Kong International Arbitration Centre
ICANN	Internet Corporation for Assigned Names and Numbers
ICC	International Chamber of Commerce
IP	intellectual property
ISP	internet service provider

IT	information technology
NRAs	National Regulatory Authorities
ODR	online dispute resolution
OECD	Organization for Economic Co-operation and Development
PECL	Principles of European Contract Law
PICC	Principles of International Commercial Contracts
PIN	personal identification number
PKI	Public Key Infrastructure
PRC	People's Republic of China
RCA	recognised certification authority
SMEs	small and medium-sized enterprises
SSL	Secure Sockets Layer
T&C	terms and conditions
TTPs	Trusted Third Parties
UCC	Uniform Commercial Code
UCITA	Uniform Computer Information Transactions Act
UCP	Uniform Customs and Practice for Documentary Credits
UDRP	Uniform Domain Name Dispute Resolution Policy
UETA	Uniform Electronic Transactions Act
UNCITRAL	United Nations Commission on International Trade Law
UNIDROIT	International Institute for the Unification of Private Law
US	United States
WIPO	World Intellectual Property Organization

Acknowledgements

高山无坦途, 沧海有驚浪 – 'there is not always smooth path for climbing up a high mountain, so does sailing'. This is the motto – an elegant Chinese classic poem that I wrote as a piece of silk-papered calligraphy when I was 18 years old. That piece of art won me a prize in the university as the strength and features of the writing reflects the writer's strong belief.

I must appreciate my parents' wisdom that they spotted my potential talents and inner determination when I was very little. They gave me endless mental, intellectual and material support, taking me to extra piano lessons, swimming and English courses to fully cultivate my mind. Their professional leadership within our society also influenced me and created a great model for me.

I am truly grateful for the support from the two profound and respected legal scholars, Professor Rob Merkin at the University of Southampton and Professor Angelo Forte at the University of Aberdeen. I can't express how much their recognition of my PhD work means to me – it really gave me so much courage and strength to move forward and continue contributing my best to the global legal society.

Last, but not least, I would like to thank my publishers, Ms Katie Carpenter and Ms Khanam Virjee for their professional and efficient work, and their friendship and support during the whole reviewing and publishing process.

Preface

The continuing innovation of information technology and ever-increasing use of the internet make international commercial transactions quicker and easier. Geographical distance no longer remains an obstacle in communications among businesses and individuals as product information can be accessed instantly via companies' websites. Taking advantage of the speed, efficiency and reduced costs of online commerce, international trade and domestic sale have been increasingly conducted over the internet for the last decade. This is beneficial for the growth of global economy but, at the same time, challenges the existing laws with newly-generated legal issues such as the validity of electronic contracts, the protection of data privacy rights and the settlement of e-disputes. In recent years international conventions and model laws, regional directives and regulations, as well as national laws have been making efforts to enhance the legal certainty of electronic commercial transactions with the primary aim of building users' confidence in online interactions and transactions.

Law of Electronic Commercial Transactions: Contemporary Issues in the EU, US and China takes a 'solutions to obstacles' approach and evaluates various contemporary key legal issues of electronic commercial transactions by comparing current legislative frameworks in the EU, US, China and international organisations. It provides in-depth research into finding solutions to modernising and harmonising laws in international electronic commerce. It promotes the establishment of well-balanced area-specific international instruments, which enhance particularised areas such as the effectiveness of electronic offer and acceptance; conditions of error in electronic communications; rules of electronic battle of forms; recognition of domestic and foreign certificates and electronic signatures; self-regulation of internet privacy policies; as well as measures of cross-border internet jurisdiction, choice of law and alternative dispute resolutions.

This book is a research monograph providing guidance for readers to understand the legal challenges of e-commerce; find practical solutions to create trustworthy online commercial platforms; and ensure security of online transactions. The real-life examples, such as Microsoft Outlook – recall or replace a message; eBay – e-trading platform and online dispute resolutions; Facebook with TRUSTe – data privacy program, have been given to advise business and individual e-commerce practice.

Part I

Introduction

1 The business and legal landscape of electronic commercial transactions

> The customer pays his money and gets a ticket. He cannot refuse it. He cannot get his money back. He may protest to the machine, even swear at it. But it will remain unmoved. He is committed beyond recall. He was committed at the very moment when he put his money into the machine.
>
> Lord Denning, *Thornton v Shoe Lane Parking*[1]

With the advent of electronic means of communication and information transfer, business deals are fast becoming conducted over the internet, taking advantage of the speed, efficiency, and cost benefits of electronic technologies. Clicking the icon of 'I agree' to make a purchase on the web page may have the same effects as 'money machines'. In a split second it may constitute a valid form of consent between two parties in different countries.

In China, the 23rd Statistical Survey Report on the Internet Development of January 2009 estimated that the amount of users of online shopping in China had reached 74 million, with an annual growth rate of 60%.[2]

In the US, the US Department of Commerce E-Stats Report was released on 28 May 2009, stating that:

> manufacturers and merchant wholesalers (so called 'B2B') accounted for most e-commerce (93%). E-commerce accounted for $1,856 billion of manufacturing shipments in 2007, up from $1,567 billion in 2006, an annual increase of 18.4%. US merchant wholesalers reported total e-commerce sales of $1,226 billion in 2007, up from a revised $1,194 billion in 2006 – an annual increase of 2.7%. US retail e-commerce sales reached almost $127 billion in 2007, up from a revised $107 billion in 2006 – an annual gain of 18.4%. From 2002 to 2007, retail e-sales increased at an average annual growth rate of 23.1%.[3]

For instance, eBay, the world's online marketplace, creates thousands of electronic contracts a day. It made a profit of $256 million in the first three months of 2005, up 28% on the same period in 2004, on sales of more than $1 billion.[4]

In the EU the number of internet users increased by 218.1% from 2000 to 2008, representing 61.4% of the total EU population and 18.8% of world usage.[5] The percentage of individuals who had ordered goods or services over the internet for private use rose significantly, from 22% to 34%, between 2004 and 2008. In the UK, Denmark, Germany and the Netherlands 57% of individuals had ordered goods or services over the internet for private use in 2008.[6]

The worldwide usage of the internet has changed the traditional ways of communications among individuals and businesses, which encourages the growth of the new economy.

1.1 Concepts and features

1.1.1 Internet

The internet, a base of connection for international electronic commerce, is a form of connected networks via electronic devices, i.e. computers. It can be accessed worldwide, and uses the standardised Internet Protocol Suite (TCP/IP) to transport data and messages anywhere in the world and permit communication between parties across a large distance.

Internet technology began in the 1960s. The first trans-Atlantic computer networks were linked up in the early 1970s.[7] During the 1960s and early 1990s, the internet was developed mainly for military, governmental and academic use. Only in the late 1990s, when Microsoft released Windows 98 with a full scale entry of an internet browser and server, did the internet start to be popular for commercial use. In the 2000s the internet experienced enormous growth, businesses set up websites displaying product information and providing trade platforms for goods and services, whilst individuals used email and instant messaging as well as shopping online. In the last 10 years business has been increasingly conducted over the internet, including international trade and domestic sales. In recent years the internet has been employed in various new ways, for example, social networking and dispute resolutions.

1.1.2 Electronic commerce

The phrase electronic commerce can be interpreted as 'commerce conducted in a digital form or on an electronic platform', or 'selling or buying goods and services on the Internet'.[8] The Organization for Economic Co-operation and Development (OECD) defines electronic commerce from an economic and social point of view as:

> all forms of commercial transactions involving both organisations and individuals, which are based upon the electronic processing and transmission of data, including text, sound and visual images. It also refers to the effects that the electronic exchange of commercial information may

> have on the institutions and process that support and govern commercial activities.[9]

In the EU the European Initiative in Electronic Commerce further describes electronic commerce as:

> any form of business transaction in which the parties interact electronically rather than by physical exchanges. It covers mainly two types of activity: one is the electronic ordering of tangible goods, delivered physically using traditional channels such as postal services or commercial couriers; and the other is direct electronic commerce including the online ordering, payment and delivery of intangible goods and services such as computer software, entertainment content, or information services on a global scale.[10]

The key words in the definition above are: commercial transactions, organisations, individuals and electronic exchange. It reveals the scope of electronic commerce from a jurisdictional and functional perspective. Electronic commerce, in a private sense, is international and domestic commerce;[11] trade[12] and business[13] for both non-personal and personal usage.

Electronic commercial transactions are one of the main components of electronic commerce which refer to deals made between either private individuals or commercial entities. Electronic commercial transactions presuppose the existence of a business transaction and create a more efficient business environment through the usage of electronic means.

There are two main types of electronic commercial transactions: business-to-business (B2B) and business-to-consumer (B2C). B2B describes trade between different businesses or entities. It can be completed by performance against payment or performance against performance.[14] B2C involves the sale of goods or services to individual customers for their own use. It is notable that in a B2C transaction one of the parties acts as a consumer. A synonymous term of B2C electronic commerce is electronic retailing.

In general, B2B provide goods or services to other businesses while B2C sells goods or services to consumers. Both forms contribute to the growth of the new economy, although B2B currently generates a larger portion of a country's GDP (gross domestic product).

1.2 Benefits: economic and social impacts

The invention of electronic commerce has been beneficial to the global economy and society. It is an innovation in conducting business that changes the habits of business entities and individuals gradually and largely. Instead of travelling a long distance to visit a shop or a factory, buyers can use a laptop with wireless internet access to enter a digital platform of buying and selling online. Buyers can surf the websites, choose products and make web

payments. As a result of successful electronic transactions individual goods will be delivered to the buyer's door or large trading containers will be shipped to the port of named destination. The profound impact of electronic commerce in the global economy and society results from the decrease in the seller's and buyer's distance and the simplification of the process of shopping or trading. Such an e-trading system will undoubtedly improve economic efficiency, competitiveness and profitability.

The second edition of the International Chamber of Commerce (ICC) Global Action Plan for Electronic Commerce in 1999 highlighted the benefits to countries within such an e-commerce environment:

1 increase internal organisational and management efficiency;
2 increase transaction efficiency and reduce transaction costs for both suppliers and buyers;
3 extend market reach of suppliers and increase choice for both suppliers and consumers;
4 provide accurate information to improve service delivery such as in health provision or the provision of information to consumers.[15]

Most of the expected benefits above have been approved during the last 10 years. In the Ministerial Meeting of the Organization for Economic Co-operation and Development (OECD), a Statistic Profile was published in June 2008 forecasting the future of the internet economy. The statistics show that the internet would change the traditional behaviour of businesses and consumers and open new market opportunities, although concerns about security, trust and privacy are still preventing a large number of internet users from buying online, for example:

a there are about 542 million hosts connected to the internet worldwide in 2008, 13 times more than in 1999;
b in 2007 an average of 95% of medium and large businesses in OECD countries were using the internet;
c between 1995 and 2006, growth in gross value added (GVA) was higher in the ICT sector (76%) than in the whole business sector (66%);
d in the EU over 30% of internet users do not buy online because of security concerns.[16]

The statistics above also prove that electronic commerce has developed quickly and is gradually becoming a dominant form of business performance. It provides companies, in particular small and medium-sized enterprises (SMEs), with lower market entry costs and the ability or possibility to extend geographic reach to a much larger market. It moves traditional commercial society from an industrial economy, where machines dominated productivity, to an information based economy where intellectual content is the dominant source of value added without geographic boundaries.

Electronic commerce will continue to play its important role in modern society improving commercial connections between enterprises and individuals at national, regional and global levels, it will stimulate internationalisation and globalisation of economy and production by creating opportunities for the free movement of goods, services, money, people, technology, information and communication, and generate new challenges for potential market growth in the future.

International harmonisation of regulations or laws for a global electronic commercial market will be crucial to the free flow of information as well as the safety of electronic commercial transactions and other data-related online activities. In addition, a consistent global standard of law in relation to electronic commerce will be one of the fundamental elements of building users' trust and confidence in conducting business, socialising or sharing information online.

1.3 The legislative approaches

1.3.1 Global regimes

Subject matters in the field of electronic commerce are very broad, covering security, privacy, data protection, etc. Confronting the variety of issues international organisations are making efforts to harmonise them through the heart and base of electronic commerce – which is electronic contracting and electronic signatures.

For example, the United Nations Commission on International Trade Law (UNCITRAL), the International Chamber of Commerce (ICC) and the Organization for Economic Co-operation and Development (OECD) are all participating in an emerging global debate concerning the changes that should be made to the form or substance of international commercial law to accommodate innovation in the technology of international commerce, in particular towards a global agreement on electronic contracting. Listed below is an international legislative umbrella of electronic commerce:

UNCITRAL

- Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods 2007 (hereafter E-confidence Promotion Report).

  The E-confidence Promotion Report was reviewed by the Secretariat in 2007 but published in 2009 by UNCITRAL.[17] UNCITRAL has been urged to update legal issues on the international use of electronic authentication and signature methods because the existing instruments which were promulgated a long time ago need to be better equipped to deal with the current development of the information society. The UNICTRAL Model Law on Electronic Commerce was adopted almost 10 years ago and the Model Law on Electronic Signatures has also been adopted for

over 10 years. The E-confidence Promotion Report serves as an explanatory note or complementary to the two Model Laws as well as the more recent instrument – United Nations Convention on the Use of Electronic Communications in International Contracts. Its aim is to remove the legal and technical obstacles to the recognition of cross-border use of electronic signature and authentication methods by introducing the criteria on a technically neutral level.

- UN Convention on the Use of Electronic Communication in International Contracts 2005 (hereafter the UN Convention)
- UNCITRAL Working Group IV (Electronic Commerce) began its deliberations on electronic contracting at its 39th session (New York, 11–15 March 2002). The UN Convention,[18] a technologically neutral approach, was adopted by the General Assembly on 23 November 2005 'to facilitate international trade by removing possible legal obstacles or uncertainty concerning the use of electronic communications in connection with the formation or performance of contracts concluded between parties located in different countries'.[19] With the aim of 'enhancing legal certainty and commercial predictability' in cross-border electronic commercial contracts it addresses issues such as the validity of electronic communication, the location of parties, the time and place of dispatch and receipt of electronic communication, the use of automated message systems for contract formation and the availability of contract terms and errors in electronic communications.[20] The provisions suggest the international standard of online contracting, which stimulate the progress of the harmonisation of national laws.
- UNCITRAL Model Law on Electronic Signature 2001
  The Model Law on Electronic Signatures,[21] a technology-neutral approach, was adopted by UNCITRAL on 5 July 2001. It avoids favouring the use of any specific technical product.[22] This approach achieves legal neutrality by granting minimum recognition to most authentication technologies, while at the same time incorporating provisions for an authentication technology of choice.[23] As stated in Article 12(2) and 12(3) of the Model Law on Electronic Signatures, a certificate or electronic signature issued outside the domestic jurisdiction will be legally effective if it offers a 'substantial equivalent level of reliability'. It generates a developed legal framework for certificate service provision within an international operative public key infrastructure (PKI) and promotes the progressive harmonisation and unification of measures and policies on e-signature issues.
- UNCITRAL Model Law on Electronic Commerce 1996
  The Model Law on Electronic Commerce,[24] a minimalist approach, was adopted by UNCITRAL on 12 June 1996. The primary motivation of the UNCITRAL Model Law on Electronic Commerce was to remove existing legal obstacles to the recognition and enforceability of electronic signatures and records. It is designed to facilitate the harmonisation of

national legislation in electronic commerce. It complements traditional international conventions and other instruments in commercial law, serving as references or interpretation in order to avoid impediments to electronic commerce. It deals with issues such as the use of modern means of electronic communications and storage of information,[25] the formation and validity of electronic contracts,[26] the legal recognition of data messages[27] and the carriage of goods.[28]

ICC

- ICC eTerms 2004
  Founded in 1919 ICC is one of the world's largest business organisations promoting trade and investment for goods and services.[29] Since the late 1990s ICC has contributed to the facilitation of e-business self-regulation for companies. The most recent guideline in general electronic contracting is the ICC eTerms 2004. It provides rather short but accessible terms with only two articles. One is the definition of an 'e-commerce agreement' and the other is the determination of the 'dispatch and receipt of an electronic message'.[30] The two eTerms are designed to be widely used for any contract of sale or other arrangement of goods, or services and to facilitate the procedures and use of electronic means in concluding a contract without interfering with the subject matter of the contract and any other agreed terms between the parties.
- ICC Guide for eContracting 2004
  ICC Guide for eContracting (hereafter the Guide) accompanies the ICC eTerms 2004 providing an explanatory note on questions such as: how to apply ICC eTerms 2004; what is the legal validity of ICC eTerms 2004; what are the limits of ICC eTerms 2004; who contracts on your behalf; with whom are you contracting; how to construct an electronic contract; what are technical specifications; how to protect confidentiality; and how to cope with technical breakdown and risk management.[31]
- ICC Global Action Plan for Electronic Business 2002 (3 July 2002)
  The third edition of the ICC Global Action Plan for Electronic Business, adopted in July 2002, aims to build the user's trust and confidence in online business.[32] The ICC Global Action Plan is very comprehensive and ambitious, addressing a wide scope of advanced issues in relation to electronic business and includes, but is not limited to, the legal formalities of electronic communications, online dispute resolution, jurisdiction and applicable law and digital IP rights, data protection and privacy, etc. Such a clear, big picture is of great value in providing the legal framework of electronic commerce. The subject matters raised in the ICC Global Action Plan have been further discussed and developed by different international organisations with more specific focus in recent years.

OECD

- OECD Guidelines for Consumer Protection in the Context of Electronic Commerce (1999)
  The OECD Guidelines for Consumer Protection in the Context of Electronic Commerce, approved on 9 December 1999 by the OECD Council, are designed to help ensure consumers' rights when shopping online.[33] Its principles are set to assist governments and private sectors in developing and implementing online consumer protection mechanisms without erecting barriers to trade, which includes transparent and effective protection; fair business, advertising and marketing practices; clear information about the business, the goods or services and transaction; confirmation of transactions; secure payment mechanisms; alternative dispute resolution and redress; privacy protection; and consumer and business education.[34]

The above conventions, model laws, guidelines or framework by themselves, do not have any legal effect until adopted and implemented by national legislation, but they can serve as a guide as to what might be incorporated into national or regional laws. Model laws can be adopted in full or part provisions by national and regional laws, while conventions can only be adopted in full except for the relevant clauses concerning reservation, declaration or exemption of particular parts or provisions.

1.3.2 Other regimes: EU, US and China

Meanwhile, other regimes such as the EU, US and China also have their regional or national umbrella legislation regulating the conduct of the electronic commercial market in order to promote regional or domestic economy.

The European Union (EU)

- The EC Directive on Electronic Commerce 2000
  The EC Directive on Electronic Commerce[35] plays an important role in regulating electronic transactions in the internal market between Member States. It provides a clear and general framework to enhance the legal certainty of electronic commerce, stimulate the efficiency of e-commerce transactions and ensure the free movement of information society services in the internal market between Member States. The main provisions of the EC Directive on Electronic Commerce are transparency obligations on operators in commercial communications; the validity of electronic messages; and limitations of liability of intermediary service providers.
- The EC Directive on Electronic Signatures 1999
  The EC Directive on Electronic Signatures[36] establishes a legal framework for the recognition of electronic signatures and the conditions of certification service within the Member States, while at the same time it

ensures the proper functioning of the internal market.[37] It promotes cross-border electronic commercial transactions between Member States by recognising the equivalent function of electronic signatures to hard-written signatures. Safety of doing business online is also protected by introducing secured technology measures. No substantial rules are given with regard to 'legal obligations where there are requirements as regards form prescribed by national or Community Law', as the EC Directive on Electronic Signatures is not meant to 'affect rules and limits, contained in national or Community law, governing the use of documents'.[38]

The United States (US)

- The Uniform Electronic Transactions Act (UETA) 1999
  The UETA, promulgated in July 1999, is a model code which has been widely adopted by 48 states and the District of Columbia.[39] It addresses electronic transactions generally with a set of uniform rules governing electronic commerce transactions without changing any applicable substantive laws.[40] Parties are allowed to opt out of part of the UETA if pre-agreed – this will not affect the legal effect of electronic transactions in the same way as paper transactions.
- The Uniform Computer Information Transactions Act (UCITA) 1999
  UCITA, initially originated from a proposal for a new UCC Article 2, was approved as a legislative model by the National Conference of Commissioners on Uniform State Laws (NCCUSL) on 29 July 1999. It is not widely adopted and has only been signed and enacted by two states: Maryland and Virginia.[41] The UCITA is a lengthy 'uniform commercial code' for software licences and other computer information transactions. It provides a number of substantial and comprehensive rules such as digital signatures, electronic records, electronic agents, licensing computer information and storage devices, etc.[42] The UCITA does not govern contracts, even though they may be licensing contracts, for the traditional distribution of movies, books, periodicals, newspapers, or the like.[43]
- The Electronic Signatures in Global and National Commerce Act (ESIGN Act) 2000
  The ESIGN Act, a technology-neutral approach, was signed by President Clinton on 30 June 2000. The ESIGN Act was enacted, in part, to promote consistency and certainty regarding the use of electronic signatures in the US and also to facilitate cross-border electronic commercial transactions. It includes several key provisions concerning the validity requirements for electronic signatures, electronic contracts and electronic records or retention requirements for electronic contracts and goods.

China

- The Law of the People's Republic of China on Electronic Signatures (China Electronic Signatures Law) 2005

The Law of the People's Republic of China on Electronic Signatures was passed by the Standing Committee of the 10th National People's Congress on 28 August 2004.[44] It entered into effect on 1 April 2005. This is the first single piece of legislation in China directly regulating the field of electronic commerce. The context of the China Electronic Signatures law has been influenced by the UNCITRAL Model Law on Electronic Commerce and the UNCITRAL Model Law on Electronic Signatures, although it is more Chinese-market-oriented. It provides a legal framework and the necessary infrastructure for the use of digital signatures. Its implementation dramatically promotes the development of the e-business market in China as it boosts users' confidence in online trading and shopping online. The structure and provisions of the China Electronic Signatures Law are similar to the UNCITRAL Model Laws. It regulates the validity and legal effect of electronic signatures and maintains the lawful rights and interests of the relevant parties concerned.[45] It applies a functional equivalent approach to electronic signatures. Parties are also free to opt out of certain provisions of the China Electronic Signatures Law. It explicitly excludes the validity of electronic communications on certain types of agreements, such as those relating to personal relations, the transfer of real estate rights and interests and public utility services.[46]

2 Technical and legal barriers to online commerce

2.1 Contracts of sale of goods

Businesses can form contracts without ever touching a pen or shaking hands, which may cause obstacles in adopting traditional contract laws and creating trust between sellers and buyers. How to ensure that an electronic contract is valid and enforceable is one of the most important and fundamental problems of electronic commercial transactions. Because national boundaries are so easily crossed, international electronic contracting faces a patchwork of legal regimes. How to avoid, for instance, terms and conditions of an electronic contract containing exemption clauses which enable the escape of any responsibility for losses or damages arising out of electronic trading has become a core concern of the digital commercial market. Although electronic contracting offers new possibilities for efficient transactions, greater flexibility and evolutionary capabilities, it also generates new vulnerabilities to abuse and confronts the legal validity of transactions.[1]

The law of electronic commercial transactions cuts across many legal fields and categories including, but not limited to, international trade law, international business law, international commercial law, private international law, domestic or regional contract law, commercial law, tort law and consumer law. International IT lawyers must be familiar with many specialised fields of law and have expert technological knowledge.

In a broad sense the law of electronic commercial transactions is commercial law and the function of commercial law can be found in a leading English case, *Kum v Wah Tat Bank Ltd*.[2] Lord Devlin in *Kum v Wah Tat Bank Ltd* stated that: 'The function of commercial law is to allow, so far as it can, commercial men to do business in the way they want to do it and not to require them to stick to forms that they may think to be outmoded. The common law is not bureaucratic'. International commercial law is used to 'describe the totality of principles and rules, whether customary, conventional, contractual or derived from any other source that is common to a number of legal systems'.[3]

In a narrow sense, the two most common forms of electronic commercial contracts: B2B (business to business) or B2C (business to consumer) are

regulated by different substantial laws or the same laws in different respects. B2B contracts concern the international sale of goods (so called 'international trade') or domestic sale of goods (so called 'domestic trade') that are not for personal use, whilst B2C contracts refer to international and domestic retail to consumers for personal consumption. Thus, cross-border B2B contracts of sale are usually governed by international trade law and international commercial law, whereas B2C contracts of sale are usually subject to domestic commercial and consumer law.

The legal relationship amongst the various laws in the field of electronic commerce can be understood from a scope that is large to narrow: commercial law ≥ international commercial law + domestic commercial law; international commercial law or international business law > international trade law; domestic commercial law > consumer law. To implement the above laws well a knowledge of basic contract law shall be applied.

In the law of electronic commercial transactions the determination of the validity of electronic contacts will be the same in both B2B and B2C transactions. Their differences lie in the different obligations or duties of the seller and buyer, remedies for breach of contract by the seller or buyer, and determination of passing property and risk, which may be subject to different substantial laws.

2.1.1 B2B Transactions: international trade

The traditional way of conducting international trade starts when the buyer visits a trade fair, or a seller's company or factory. Then the buyer will select a product, ask for a price quotation and consult about packaging, date and methods of delivery of goods, as well as payment. If the quotation includes the price of the goods and all the fees until the transfer of goods for shipment, this kind of international sale of goods contract is known as a FOB (Free on Board) contract.

Sometimes the quotation will not only include the FOB price but also fees for freight and insurance. The seller is also required to prepare transport and insurance documents which shall be transferred to the buyer. This kind of contract is usually known as a CIF (Cost, Insurance and Freight) contract. It is argued that a CIF contract is deemed to be 'a sale of goods that is performed by the delivery of the documents' by the Court of Appeal in *Arnhold Karberg*.[4]

With the adoption of information technology, buyers nowadays may select their products from the e-catalogue on the seller's company website, negotiate the price and other conditions via electronic communications, and conclude a FOB or CIF contract over the internet.

To form a FOB or CIF contract, either online or offline, the parties shall insert a choice of law clause stating that the contract will be governed by the law of his own country or others. For example, if the parties express a term 'the contract shall be governed by English law' for the international sale of

goods, the Sale of Goods Act 1979 will apply. Or, the seller may choose the ICC standard trade terms, Incoterms 2000,[5] to govern the contract. Or, if the seller and buyer are contracting parties to the the United Nations Convention on Contracts for the International Sale of Goods (CISG) provided by the United Nations Commission on International Trade Law (UNCITRAL), they might choose CISG as the applicable law. Currently, two thirds of the countries in the world that are involved in international trade are contracting parties to the CISG 1980. Both China and the US ratified the CISG, thus, in absence of an effective applicable law clause, its 'default rules' on contract formation and performance will govern contracts for international sale of goods. However, it is notable that the UK is not a contracting party to the CISG.

As the CISG was adopted in 1980, before the boom in electronic commerce, its applicability and suitability in resolving electronic export contracts has been debated. The UN Convention, adopted in 2005, is deemed to be an international instrument that complements the CISG in the era of information society.

Firstly, the CISG and UN Convention have similarities and differences in their scope. The similarity is that both the CISG and UN Convention only apply to international B2B contracts but not contracts concluded for personal, family or household purposes.[6] The difference is that the CISG only applies to contracts of international sale of goods whose places of business are in different states, but not service between parties,[7] whereas the UN Convention applies to 'electronic communications in connection with the formation or performance of a contract between parties whose places of business are in different states' including sale of goods and service.[8]

Secondly, with regard to the issue of the validity of electronic communications, the UN Convention performs a supplementary role to the CISG in legal recognition of electronic communications as to forms, because the UN Convention explicitly recognises the legal equivalence of electronic contracts and signatures to written forms.[9] In contrast, the provisions of the validity of contract formality under the CISG must be analysed through statutory interpretation and advisory opinions in order to legitimise electronic means in contracting and signatures: Article 11 of the CISG provides that 'a contract of sale need not be concluded in or evidenced by writing and is not subject to any other requirement as to form. It may be proved by any means, including witnesses'.

In 2003 the first opinion of the CISG Advisory Council addressed the issue of the interpretation of electronic communications under Article 11 of the CISG,[10] and suggested that a contract may be concluded or evidenced by electronic communications because Article 11 of the CISG doesn't prescribe any form which enables the parties to conclude contracts electronically. However, such electronic communications should be 'retrievable in perceivable form' according to Article 13 of the CISG. This advisory opinion sets the recognition of electronic communications on the conditions and restrictions

of the possibility to save (retrieve) the message and to understand (perceive) it,[11] whilst the UN Convention adopts a functionally equivalent open approach in terms of electronic messages and electronic signatures. This should be deemed to be an improvement upon the CISG Advisory Council on the legal certainty of electronic communications.

Thirdly, the UN Convention specialises in the rules of ascertaining the location of the parties acting over the internet,[12] while Article 10 of the CISG provides limited rules for determining a party place of business without considering particularised features of the internet as follows: '(a) if a party has more than one place of business, the place of business is that which has the closest relationship to the contract and its performance, having regard to the circumstances known to or contemplated by the parties at any time before or at the conclusion of the contract; (b) if a party does not have a place of business, reference is to be made to his habitual residence'.

Fourthly, the Convention established a standard language in determining the time of dispatch and receipt of electronic communications,[13] whereas Articles 15 and 18(2) of the CISG use a term 'reach' to describe the dispatch and receipt of a message that '(1) an offer becomes effective when it reaches the offeree; (2) an offer, even if it is irrevocable, may be withdrawn if the withdrawal reaches the offeree before or at the same time as the offer'[14] as well as 'an acceptance of an offer becomes effective at the moment the indication of assent reaches the offeror'.[15] The Advisory Council of the CISG explains the term 'reach' as it corresponds to the point in time when an electronic communication has entered the offeree's server for an offer, and has entered the offeror's service for an acceptance.[16] However, it is not as precise as the wording of the time of dispatch and receipt of electronic communications under the UN Convention although the UN Convention fails to provide a substantial rule on the effectiveness of offer and acceptance (which will be discussed in detail in Part 2).

Lastly, but not least importantly, Article 14 of the UN Convention specially regulates input errors in electronic communications, which complements the general rule of error in communication under the CISG. According to Article 27 of the CISG, if any notice, request or other communication is given or made by a party in accordance with this Part and by means appropriate in the circumstances, a delay or error in the transmission of the communication or its failure to arrive does not deprive that party of the right to rely on the communication. The Advisory Council of the CISG recognises the form of electronic means in a notice, request or other communication whenever the addressee has consented to receiving electronic messages of this type expressly or impliedly, in that format, and to that address.[17] However, the Advisory Council does not explain its application on correction or withdrawal of errors in electronic communications, which have been fortunately compensated by the UN Convention to some extent.

2.1.2 B2C Transactions: consumer contracts

As mentioned earlier, B2C contracts are identical to B2B contracts in terms of the determination of the validity of electronic contracts, the time and place of dispatch and receipt of electronic communications and the location of the parties. However, the differences arise between the two types of contracts because consumers are the weaker parties in commercial transactions and they need particularised rules to protect their rights. Special rules equipped to the protection of consumer rights shall include consumer information, liability of inconformity of supplied goods or service, time and burden of proof and remedies. Other substantial special areas such as unfair contract terms, security and privacy shall also be specified to protect consumer rights.

Consumer rights are usually protected by national or regional consumer laws only, while B2B contracts may be governed by either international commercial law or domestic law. For example, the Sale of Goods Act 1979 applies to international sale of goods when parties choose English law as the applicable law in the contract of the sale of goods. Meanwhile, the Sale of Goods Act 1979 also protects UK consumers' rights according to the general provisions and additional rights of the buyer in consumer cases. According to Article 48B and 48C of the Sale of Goods Act 1979, where there is any breach of implied terms as to description, satisfactory quality or fitness for purpose, the buyer as a consumer may have the right to require the seller to repair or replace the goods, or reduce the purchase price of the goods, or rescind the contract.

On 8 October 2008 the European Commission adopted the proposal for a Directive on Consumer Rights.[18] It aims to update and modernise existing consumer rights, bringing them in line with technological change and strengthening provisions in the key problem areas.[19] At the same time, it also remains compatible with other new regional instruments; for example, the provisions of this new Directive should be without prejudice to Regulation (EC) No 593/2008 of the European Parliament and of the Council applicable to contractual obligations (Rome I).[20]

The proposal of the EC Directive on Consumer Rights simplifies and merges four existing EU consumer directives into one set of rules. They are: EC Directive on Sale of consumer goods and guarantees (99/44/EC); EC Directive on Unfair contract terms (93/13/EC); EC Directive on Distance selling (97/7/EC); EC Directive on Doorstep selling (85/577/EC). The new Directive should ensure a high level of consumer protection, establish the real retail internal market and make it easier and less costly for traders to sell cross-border and provide consumers with a larger choice and competitive prices. For example, Chapter I of the proposal of the EC Directive on Consumer Rights contains common definitions such as 'consumer' and 'trader' and lays down the principle of full harmonisation. Chapter II governs the rules of consumer information, information to be provided by

traders prior to the conclusion of all consumer contracts as well as information obligations on intermediaries concluding contracts on behalf of consumers. Other chapters deal with consumer information and withdrawal rights for distance and off-premises contracts, other consumer rights specific to sales contracts and general provisions concerning enforcement and penalties.

The proposal of the EC Directive on Consumer Rights is specially geared to the needs of the information society. Article 11 of the Proposal of the EC Directive on Consumer Rights designates the formal requirements for distance contracts. Article 14 further details that 'for distance contracts concluded on the Internet, the trader may, in addition to the possibilities referred to in paragraph 1, give the option to the consumer to electronically fill in and submit the standard withdrawal form on the trader's website. In that case the trader shall communicate to the consumer an acknowledgement of receipt of such a withdrawal by email without delay'.

The Proposal of the EC Directive on Consumer Rights controls unfair contract terms both offline and online with explicitly detailed rules. It adopts a wide cooling-off period of 14 calendar days when consumers can change their mind and withdraw the contract using a standard withdrawal form. It maintains the principle that the trader is liable to the consumer for a period of two years if the goods are not in conformity with the contract and entitles consumers to ask for repairmen, replacement and guarantees of goods and services.

In general, the proposal of the EC Directive on Consumer Rights seems to have reasonable and considerable provisions to balance a high level of consumer protection and the competitiveness of enterprises, enhance consumer confidence in the internal market and reduce business reluctance to trade cross-border.

2.2 Contracts of carriage of goods

An essential difference between contracts of sale of goods and contracts of carriage of goods lies in terms of liability and documentation.

Compared with B2B international contracts of carriage of goods, in B2C contracts, when delivery of goods is required, the material possession of the goods shall be transferred to the consumer or to a third party, rather than a carrier. Rules of delivery in B2C contracts are usually governed by domestic commercial law or consumer law, which is the same law that governs contracts of sale of goods for personal, family, and household purposes.

In B2B contracts, shipment or transportation of goods by sea is deemed to be one of the methods of delivery of goods. A bill of lading is a document issued to a shipper of goods (usually the seller but possibly the buyer) by a shipowner, performing as a contract of carriage of goods with terms and conditions as well as the description of goods that have been loaded on board. The definition reflects the three functions of a bill of lading: firstly, it is evidence of the contract of carriage, because the terms and conditions set out

on the reverse of the bill of lading are governed between the shipper and carrier.[21] Secondly, it acts as a receipt for the goods that have been loaded on board, because the bill of lading contains a description of the goods. When the shipowner confirms that the goods received are in 'apparent good order and condition', he or she will issue a 'clean' bill. When this statement is qualified, the bill is 'claused'.[22] Thirdly, it is a document of title, because possession of a bill of lading is in many respects equivalent to possession of goods, although it is symbolic.[23]

Often a more informal document, rather than a bill of lading, is given to the shipper when the goods are loaded on board. This is known as a mate's receipt. The details on the mate's receipt are then inserted into a bill of lading which is given to the shipper before the ship leaves the port of loading.

One of the principal purposes of the bill of lading is to enable the owner of the goods to resell them rapidly although the goods are not in his hands but are in the custody of a carrier. For example, when goods are on the high seas in transit from London to Hong Kong, the bill of lading will be passed to the buyer in Hong Kong and the buyer will thus become the owner of the goods. The bill of lading representing the goods enables the buyer to promise the goods with his bank in Hong Kong or to resell them elsewhere in the world.

A traditional bill of lading is a piece of paper which would be physically delivered or faxed. International trade is now making extensive and increasing use of information technology to facilitate cross-border trade. Nowadays, in the shipping industry, traditional paper-based shipping documents, in particular bills of lading, are gradually being replaced by paperless bills to improve the speed and efficiency in international transactions. However, there are a number of obstacles to the use of electronic bills of lading, both in terms of technological and legal issues.

One of the most prominent shortcomings of a traditional bill of lading is that it is a piece of paper which may be copied or written incorrectly by negligence, or easily forged. Very often the delivery of a paper-based bill of lading may cause delay. It is usually ready for the shipper to pick up from the carrier the day after the vessel sails, but the average delay before the paper document is ready is three days.[24] Moreover, a paper-based bill of lading may not be easily kept and protected. However, in an electronic environment, although the speed and efficiency of bills of lading is improved, the challenge is to preserve and secure electronic records that replicate paper data, and to ensure their authentic, unique, and confidential nature so as not to diminish confidence in the information system. In addition it is challenging to implement electronic bills of lading because of the divergent documentary practices of carriers, bankers and shippers.

There are a number of international instruments that make efforts in paving the way for the recognition and implementation of electronic transport documents. They are mainly:

- The Committee Maritime International (CMI) Rules for Electronic Bills of Lading in 1990;
- UNCITRAL Model Law on Electronic Commerce in 1996;
- United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea – the 'Rotterdam Rules' in 2008.

CMI Rules for Electronic Bills of Lading 1990

The Committee Maritime International (CMI) adopted Rules for Electronic Bills of Lading in 1990. The CMI Rules are voluntary so they will apply only if the parties to a contract of carriage agree so; the Rules then operate by incorporation into the contract. The CMI Rules provide for a private registry system for electronic messages as bills of lading, as stated in Article 4 of the CMI rules:

a. The carrier, upon receiving the goods from the shipper, shall give notice of the receipt of the goods to the shipper by a message at the electronic address specified by the shipper.
b. This receipt message shall include:

   (i) the name of the shipper;
   (ii) the description of the goods, with any representations and reservations, in the same tenor as would be required if a paper bill of lading were issued;
   (iii) the date and place of the receipt of the goods;
   (iv) a reference to the carrier's terms and conditions of carriage; and
   (v) the Private Key to be used in subsequent Transmissions.

   The shipper must confirm this receipt message to the carrier, upon which Confirmation the shipper shall be the Holder.
c. Upon demand of the Holder, the receipt message shall be updated with the date and place of shipment as soon as the goods have been loaded on board.
d. The information contained in (ii), (iii) and (iv) of paragraph (b) above including the date and place of shipment if updated in accordance with paragraph (c) of this Rule, shall have the same force and effect as if the receipt message were contained in a paper bill of lading.

From the essence of the CMI Rules it is notable that digital signatures are adopted in encrypting and authenticating electronic bills of lading. Traditionally a paper-based bill of lading passes from trader to trader, retaining its identity as a single document, and not returning to the carrier until the goods are discharged, whereas an electronic bill of lading returns to the carrier every time it is negotiated, and each successive trader is effectively issued a new document transmitted from the ship. The function of paper-based bills of

lading is incorporated in electronically generated documents. However, there are some disadvantages of the CMI rules in that there is no provision for the transfer of contractual rights and liabilities along with the documentation; there are also no remedies for non-payment against electronic bills of lading; and there is no provision for determining the passing of property in the goods.[25]

UNCITRAL Model Law on Electronic Commerce 1996

The UNCITRAL Model Law on Electronic Commerce, adopted in 1996, not only provides general provisions to the recognition of electronic communications, but also special provisions to actions related to carriage of goods and transport documents in electronic commerce. Both Articles 16 and 17 of the Model Law on Electronic Commerce contain provisions that apply to the transfer of rights in goods by electronic means. Article 16 establishes functional equivalents of written information about actions related to the carriage of goods, whereas Article 17 creates functional equivalents of the performance of such actions through the use of paper documents.[26]

The special provisions of the Model Law on Electronic Commerce confirm the legal effect in electronic transport documents but give the broad scope of application without providing any substantial rules. Specialised international and national laws concerning carriage of goods still need to be employed to deal with substantial issues. For example, at the international level, there is the United Nations Convention on the Carriage of Goods by Sea 1978 – the 'Hamburg Rules' (implemented in 1992) – however, the UK did not ratify the Hamburg Rules. Thus, in the UK, the Carriage of Goods by Sea Act 1971, implementing the 'Hague-Visby Rules', will govern the contract of carriage of goods by sea.

UN Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea – the 'Rotterdam Rules' in 2008

The current legal regime governing the international carriage of goods by sea lacks uniformity and fails to adequately take into account modern transport practices, in particular, electronic transport documents. Since 2002, UNCITRAL has tried to create a modern and uniform law concerning the international carriage of goods by sea.

The UN Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea (the Rotterdam Rules), adopted by the General Assembly on 11 December 2008,[27] provides a uniform and modern regime for the international carriage of goods by sea. It builds upon, and provides a modern alternative to, three earlier main conventions on the international carriage of goods by sea. They are: the International Convention for the Unification of Certain Rules of Law relating to Bills of Lading (Brussels, 25 August 1924) (the Hague Rules), and its Protocols (the Hague-Visby

Rules), and the United Nations Convention on the Carriage of Goods by Sea (Hamburg, 31 March 1978) (the Hamburg Rules).

One of the main achievements of the Rotterdam Rules is that they facilitate electronic transport documents in contracts for the international carriage of goods by sea. Article 1 of the Rotterdam Rules gives clear definitions of 'electronic communication', 'electronic transport record', 'negotiable electronic transport record' and 'non-negotiable electronic transport record'. The definition of 'electronic transport record' is the essence of the Rotterdam Rules. Article 1(18) provides clearly and precisely that:

> Electronic transport record means information in one or more messages issued by electronic communication under a contract of carriage by a carrier, including information logically associated with the electronic transport record by attachments or otherwise linked to the electronic transport record contemporaneously with or subsequent to its issue by the carrier, so as to become part of the electronic transport record, that: (a) evidences the carrier's or a performing party's receipt of goods under a contract of carriage; and (b) evidences or contains a contract of carriage.

The above definition reveals the two main functions of 'electronic transport record': one is evidence of receipt of goods and the other is evidence of contract of carriage. Article 3 further confirms the effectiveness of electronic communications and that electronic communication shall be adopted with the consent of the person by which it is communicated and of the person to which it is communicated.

Moreover, Chapter 3 (including Articles 8–10) of the Rotterdam Rules is in charge of the recognition and procedures for the use of 'electronic transport records', which has a similar condition described in Article 3 that the validity of 'electronic transport records' is subject to the consent of carrier and shipper. Chapter 8 (Articles 35–42) of the Rotterdam Rules governs the effectiveness of contract particulars in 'transport documents and electronic transport records'. The form requirements of electronic signatures and authentication are set in Article 9 impliedly and in Article 38 explicitly.

The Rotterdam Rules are different from the other international conventions as they incorporate the term 'electronic transport records' in general provisions parallel to the term of 'transport documents' (which means paper transport documents) throughout the whole convention, whereas most of the other conventions with non-specific electronic commerce subject matters will normally recognise the validity of electronic communications with the functional equivalent rule in one single provision, but leave the other provision with the traditional wording of paper-based documents or transactions. The Rotterdam Rules 2008 should be deemed to be one of the most updated uniform and modern conventions that supports the efficient usage of electronic means in the shipping industry.

2.3 Electronic payments

Electronic payments can be understood as paying for goods or services via electronic means rather than by cash. It includes a large variety of forms. In B2C electronic commercial transactions it is most common that consumers pay the product fees online using their credit cards or debit cards. In B2B electronic trading transactions electronic letters of credit (known as 'documentary credit') are the most popular method to pay for goods against bills of lading.

B2C electronic payments, also known as internet payments, are fast and convenient, but sometimes the security of using online payments is challenged. Often when consumers proceed with a payment on the internet online merchants will only request the credit card or debit card numbers and billing addresses. Credit card numbers are at risk of being stolen or kept by online merchants for unauthorised use, as are the billing addresses. Although consumers' billing addresses may change, new billing addresses can ordinarily be obtained from a public telephone book or internet database. Thus, security and privacy protection is one of the major concerns of shopping online. It is estimated that over 30% of internet users do not buy online because of security concerns in the EU.[28] To build up consumers' confidence and facilitate online retailing, national, regional and international organisations have made efforts to promulgate rules in data privacy protection in recent years. This issue will be discussed in detail in Part III.

In B2B trading contracts the exporter and the overseas buyer usually agree in the contract of sale that payment will be made under a letter of credit. Next, the overseas buyer (applicant) instructs a bank at his place of business (issuing bank) to open a letter of credit for the exporter (beneficiary) on the terms specified by the buyer in his instructions to the issuing bank. Then, the issuing bank arranges with a bank at the locality of the exporter (advising/confirming bank) to negotiate, accept, or pay the exporter's draft upon delivery of the transport documents – bills of lading by the seller. Finally, the advising/confirming bank informs the exporter that it will negotiate, accept or pay his draft upon delivery of the transport documents.

There are two fundamental principles of using letters of credit: one is the autonomy of the credit; and the other is the doctrine of strict compliance. With regard to the principle of autonomy of the credit, the letter of credit is separate from and independent of the underlying contract of sale or other transaction. In other words the letter of credit is for the exchange of the documents but not for the goods.[29] This can be evidenced by a land-marking case *Power Curber International Ltd v National Bank of Kuwait*.[30] In this case distributors in Kuwait (buyer) bought machinery from Power Curber (seller), an American company carrying on business in North Carolina. The National Bank of Kuwait issued an irrevocable letter of credit, instructing the Bank of America in Miami to advise the credit to the sellers through a bank in Charlotte, North Carolina. The machinery was duly delivered but the

Kuwaiti buyers raised a large counterclaim against the sellers in the courts of Kuwait and the bank, which was willing to honour the irrevocable credit. The judge held: 'it is vital that every bank which issues a letter of credit should honour its obligations. The bank is in no way concerned with any dispute that the buyer may have with the seller'.

The second principle – the doctrine of strict compliance – means that the bank is entitled to reject documents which do not strictly conform with the terms of the credit. For example in the case of *Soproma SpA v Marine & Animal By-Products Corporation*,[31] the buyers, an Italian company, bought a quantity of Chilean Fish Full Meal from a New York company. The documents to be presented by the sellers to the bank had to include bills of lading issued to order and marked 'freight prepaid' and an analysis certificate stating that the goods had a content of minimum 70% protein. The sellers tendered to the advising bank in New York bills of lading which did not bear the remark 'freight prepaid' but, on the contrary, bore the remark 'collect freight'; the analysis certificate showed only a protein content of 67% minimum; and the goods, although described in the invoice as 'Fish Full Meal', were described in the bills of lading only as 'Fishmeal'. The court decided that the buyers had rightly rejected the documents.

The Uniform Customs and Practice for Documentary Credits (UCP) is a successful international instrument standardising banking practice relating to letters of credit, issued by the International Chamber of Commerce (ICC). The first version for the UCP rule was published in 1933, and the most recent version known as UCP 600, the seventh version of the rules, was published on 1 July 2007. Bankers, traders, lawyers, transporters, academics and all who deal with letters of credit will refer to UCP 600. To facilitate the use of electronic means of issuing and responding to letters of credit, the eUCP (Version 1.1) was launched by the ICC as a supplement to the UCP in order to accommodate presentation of electronic records alone or in combination with paper documents.[32] According to Article 8 of the eUCP, any requirement of the UCP or an eUCP credit for presentation of one or more originals or copies of an electronic record is satisfied by the presentation of one electronic record.

2.4 Dispute resolutions

A good international long-term business relationship is crucial for the maintenance and further development of the business of enterprises. Forming and keeping an ongoing healthy international business relationship requires businessmen's interpersonal communication and negotiation skills and more importantly, demands businessmen's professionalism and maturity in dealing with business disputes. Going to the courts straight away whenever international trade disputes arise is not a very wise decision as cross-border litigation takes a long time, involves high litigation fees and consumes a large amount of time. A sophisticated contract of international sales will usually

have a dispute resolution clause. In such a clause alternative out-of-court methods of dispute settlement, known as alternative dispute resolution (ADR) including arbitration, mediation and negotiation are more frequently employed. Arbitration is the most common way of dealing with large claims in international trade.

In the information society contracts, transport documents and payments of international trade are communicated, generated and issued by electronic means. In other words most of the evidence is in digital form. Resolving disputes online seems to be logical due to the access to digital evidence and the avoidance of cross-border travel. Such methods are introduced as online dispute resolution (ODR). ODR is the equivalent to electronic alternative dispute resolution and cybercourt, but moving traditional offline dispute resolution and litigation online. It has been a new, challenging and much researched issue since the mid 1990s. Its occurrence will boost confidence in doing business online and will certainly be more efficient than offline methods in cases that have an 'international' or 'cross-border' factor. However, there are barriers in promoting ODR globally because of the lack of an international harmonised standard for ODR service practices and the incompatibility of the level of ODR legal and technological experts as well as facilities in different countries. The most updated practical and legal issues of ODR will be discussed and evaluated in Part IV.

Summary

The exponential growth of electronic usage in global commercial transactions has created new challenges to existing laws. Some of the legal solutions still lag behind because of the unique complexities attached to electronic commerce. In order to encourage electronic commerce, efforts to reform or establish international commercial laws may be needed to make them suitable to different cultures, economies and policies, comprehensive and practical to enable safe cross-border trading, sufficiently open to the upgrading technology innovations, and manageable in order to build up e-trust and e-confidence.

In analysing and evaluating these matters this book focuses on the common legal issues in B2B and B2C electronic commercial transactions, surveys the comparative electronic commerce statistics, and compares the legislative frameworks in the EU, US, China and international organisations in general. It then provides an in-depth research into firstly, validity and formation of electronic contracting; secondly, electronic signatures and authentication; thirdly, data privacy protection; fourthly, jurisdiction and choice of law issues in electronic contracting; fifthly, online dispute resolutions, and finally, proposes recommended solutions to overcoming the obstacles to electronic commercial transactions. It aims to create a harmonised international practical legal approach for electronic commercial transactions and dispute resolutions.

The structure of the whole book adopts an 'obstacles and solutions' approach. This book first asks what the barriers to electronic commercial transactions are, and answers those questions by finding the solutions. There are eight main obstacles to electronic commercial transactions:

1 What constitutes a valid electronic contract?
2 How can electronic battle of forms, automated message systems and errors in electronic communications be dealt with?
3 How can the recognition of electronic signature and authentication be ensured?
4 What can be considered as sufficient protocols to protect personal data privacy rights?
5 How can jurisdiction be determined in electronic contracts?
6 What law is applicable to electronic contracts?
7 How can disputes referring to electronic contracting be resolved and how can the decisions of online dispute resolution be enforced?
8 How can one build an infrastructure for trusted e-commerce, and thereby build trust among e-commerce customers?

According to the above issues, the book starts the discussion with electronic contracting. It is one of the most challenging and important subjects in electronic commerce, because legal certainty is the basis of building trust in doing business online. It will be based on the most current international legislation, the UN Convention on the Use of Electronic Communications in International Contracts, and it will be compared with the EU, US and Chinese relevant legislations. It will examine whether it is sufficient to merely guide the conduct of international electronic commercial contracts without resorting to mandatory, binding rules, by analysing factors such as the validity of an electronic contract, the time and place of dispatch and receipt of an electronic communication, errors in an electronic communication, and the location of parties. This also contributes to the two most debatable issues in electronic contracting: one is offer and acceptance, and the other is the battle of forms. Those two issues, unfortunately, were not included in the UN Convention and other national legislations.

After finding under what conditions an electronic contract is valid, the next focal point will be: electronic signatures and authentication as well as data privacy protection. E-signature with authentication is a security tool to ensure the safety of electronic transactions. It identifies contracting parties and their affixed documents utilising encryption. It is essential that the conduct of Certification Authorities is regulated, because the quality and trust in electronic authentication services will affect the operation of the electronic market. In most national laws both non-recognised and recognised certification authorities can provide electronic authentication services and may even have the same effects on certificates. Part III of Internet Security in the book will tackle issues such as: what constitutes sufficient signature and

authentication to secure electronic commercial transactions, what will be the liabilities of Certification Authorities, and how can the recognition of foreign certificates be ensured? How can international or regional protocols redress the balance between the free flows of data information for stimulating economic globalisation and the protection of basic human privacy rights to expedite the process of increasing trust and confidence in doing business online?

Having analysed the existence of electronic contracts alongside internet security, the next issue will move onto the application of private international law on the internet. In other words, when disputes arise, which court will have jurisdiction and whose law will be chosen? Jurisdiction, one of the oldest and most complicated issues in traditional laws, is even more complex in the online environment. When digitised goods are delivered electronically, the place of delivery is no longer physical; thus it is much more difficult to ascertain the place of delivery online than offline. So will it affect the traditional principle of determining jurisdiction? Part IV will examine general, special and exclusive jurisdiction issues by EU Brussels I Regulation, US cases and Chinese laws, and attempt to find solutions to remove obstacles to the determination of internet jurisdiction. It will also analyse the Rome I Regulation and the US and Chinese legislations through discussing two main points: one is the applicable law in cases of choice and the other is the applicable law in the absence of choice. It will comment on the improvement of the Rome I Regulation compared with the Rome Convention and criticise some unresolved issues in the Rome I Regulation which need to be further developed. The last issue in the book, but not the least, deals with online dispute resolution (ODR), which has been argued as one of the most plausible and efficient channels to enhance trust and confidence in doing business online.

Part II

Electronic contracts

The development of electronic commerce signifies that businesses increasingly rely on the internet to conduct their transactions. Undoubtedly the computer provides a useful digital platform for sellers and buyers. The formation and validity of electronic contracts is the focal point in electronic commercial transactions, which will be examined by discussing and analysing the following scenario:

The scenario of electronic contracting

Stage 1:
A buyer (B) accesses a website selling airline tickets controlled by a seller (A), an airline ticket sale company, and asks the price of return flight tickets from London to Paris. B has never had any dealings with A before. Having checked that there are flight tickets available, A's computer uses knowledge that it has acquired itself to calculate a price by means of a complex formula that it has evolved for itself. The computer then notifies B of the price at which it is prepared to sell the tickets. B responds by ordering a quantity of tickets to be dispatched to B, completes the required web form and an appropriate debit to be made from his bank account. B also scrolls through part of the agreement (standard terms and conditions) and decides to click on the button to signify assent to the terms and conditions.

Stage 2:
A never knows that this transaction has occurred. The website also does not clearly give B the knowledge of when the contract is finally concluded and B is fooled into pressing the wrong button before he is able to consider whether he wishes to be finally bound by the contract.

Stage 3:
Only after the conclusion of the contract does B realise that tax is not included in the price, and that the price is much higher than originally indicated – as the price of flight tickets has changed while the buyer was acting on the website. Meanwhile, B also realises that he has requested the

wrong quantity of tickets. Instead of booking for one person, he orders and pays for two persons.

When B discovers the pricing error he sends emails and letters to A's web-mail accounts notifying them of this error and asking for correction.

Legal concerns in response to the scenario

1 Does the above transaction constitute a valid contract?
2 When is the offer effective and when is the acceptance to the offer effective?
3 Does A have a right to amend the wrong advertisement on the website after the order has been made?
4 Is 'error in electronic communications' equivalent to 'the traditional mistake and misrepresentation in contracts'? If not, what are the differences?
5 What are the duties and liabilities of internet service providers?

The above scenario also reflects four main legal doctrines that need to be determined in order to remove the obstacles to electronic communications:

1 What is electronic contracting?
2 Who is contracting?
3 When is an electronic contract made?
4 Where is the contract made?

Firstly, at the national and international level, the directives, model laws and conventions governing electronic commercial transactions do not cover when offers and acceptances of offers become effective for purposes of contract formation.[1] Neither does the most recent international instrument – the UN Convention on the Use of Electronic Communications in International Contracts (UN Convention).[2] It is still debatable whether the UN Convention should include a provision on when an offer and acceptance in electronic form takes effect, and whether the existing rule of the time of dispatch and receipt of electronic communications will be sufficient to ascertain an offer and acceptance. If so, how should it be explained, and if not, what should be done about it?

Secondly, the UN Convention does not impose a duty of the availability of contract terms,[3] whilst the EC Directive on Electronic Commerce does.[4] The problem arises because no such obligations existed under the United Nations Convention on Contracts for the International Sale of Goods (CISG) or most of the other international instruments dealing with commercial contracts.[5] The crucial difference between paper-based and electronic contracts is that once a contract is written, if parties keep it safe, it can be stored forever, whilst a contract is concluded by electronic means without the possibility of re-accessing it again or downloading it afterwards – it might be lost forever; therefore it may become a barrier to evidential proof.

Thirdly, the UN Convention recognises that it is now possible to conclude a contract by electronic agents without any human intervention. Electronic transactions could take place either between an individual and an electronic agent acting on behalf of an individual, or between two electronic agents acting respectively on behalf of two individuals.[6] The US Uniform Electronic Transactions Act (UETA) provides that 'a contract may be formed by the interaction of electronic agents of the parties, or by the interaction of an electronic agent and an individual'.[7] It is a so-called 'automated message system'. Automated message systems, also known as 'electronic agents', refer essentially to a system for automatic negotiation and conclusion of contracts without the involvement of a person, at least on one of the ends of the negotiation chain.[8]

The UN Convention also introduces the use of automated message systems.[9] It aims to clarify that automated means of communication can convey the intention necessary in contract formation, providing that a contract shall not be denied validity or enforceability on the sole ground that: when one or both parties have interacted in the contracting process by using an automated message system without review by any person, or when a contract is formed by the interaction of two automatic message systems.[10] This is a non-discrimination rule intended to make it clear that the absence of human review of or intervention in a particular transaction does not by itself preclude contract formation.[11] The Explanatory Note of the UN Convention in 2007 explains that 'Electronic communications that are generated automatically by message systems or computers without direct human intervention should be regarded as "originating" from the legal entity on behalf of which the message system or computer is operated'.[12] The EC Directive on Electronic Commerce and the UNCITRAL Model Law on Electronic Commerce lack specific rules on that matter. Although the UN Convention has significantly recognised automated message systems, there is a query about whether the rules of an automated message system would conflict with the consent requirements of concluding an e-contract, if 'consent' between two contracting parties is agreed as a prerequisite of forming a contract.

The fourth obstacle, which connects to the first and the third obstacles above, is error in electronic communication. Article 14 of the UN Convention addresses a type of error specific to e-commerce, namely data input errors, in view of the potentially higher risk of error in real time or near instantaneous communications made between individuals and automated systems. It deals with the consequences of errors made in interactions between individuals and automated information systems that do not offer the individual an opportunity to review and correct the input error. It requires a party offering goods or services through an automated information system to make available some technical means of identifying and correcting errors. It makes sense that consent may be required prior to the conclusion of an automated e-contract system, because meanwhile, it makes time available for error amendments.

The penultimate obstacle is the determination of the location of parties.

Unlike the offline world where parties have physical venues, the online business can be located only in space. Therefore, how to determine the location of parties who are doing business online becomes a debated issue. There is no specific provision governing this issue under directives or model laws on electronic commerce; however, the UN Convention has established a provision in an attempt to remove the uncertainty of determining the location of parties. It is still doubted whether this provision under the UN Convention is sufficient and practical.

Finally, battle of forms, which is the most complicated issue in commercial contracts, raises barriers to offline contracting. Electronic contracts add another, more difficult, element into this dimension. Whether the existing international instruments dealing with battle of forms are adequate with regard to the battle of electronic standard contracts must be examined.

The solutions to the obstacles in electronic contracting as illustrated above will be proposed in the following chapters, mainly answering the following questions:

1 What is electronic contracting?
2 Who is contracting?
3 When is an electronic contract made?
4 What are the remedies when errors in electronic communications occur?
5 Where is an electronic contract made?
6 How can electronic battle of forms be dealt with?

3 What is an electronic contract?

3.1 The definition of electronic contracting

The ICC refers to 'electronic contracting' as 'the automated process of entering into contracts via the parties' computers, whether networked or through electronic messaging'.[1] This definition is an amalgamation of two separate explanations, one contained in the UN Convention[2] defining 'electronic communication', and the other taken from the US UETA and UCITA providing for 'automated transactions'. 'Electronic communication' means 'any communication that parties make by means of data messages',[3] whereas 'automated transactions' means any transaction conducted or performed, in whole or in part, by electronic means or electronic records. In addition, electronic communication establishes a link between the purposes for which electronic communications might be used, and the notion of 'data messages' which was important to retain.[4] This new concept gives a broader definition of electronic means of transactions and makes it compatible with a wide range of possible developing techniques.

3.2 Features: email v. clickwrap v. shrinkwrap

The UNCITRAL Model Law on Electronic Commerce states that 'an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose'.[5]

There are two main ways in which commercial contracts can be made electronically. A common and popular method is through the exchange of electronic mail (email). Email can be used to make an offer and to communicate an acceptance of that offer. The email containing the offer or acceptance can be sent through the offeror's (or offeree's) outbox, the digital equivalent of a postbox, to a server of an internet service provider (ISP) and then forwarded to the offeree's (offeror's) inbox. The other method of contracting is using the world wide web. Normally, the vendor would provide a display of products on his website and indicate the cost of such products. A customer

can scroll through the website previewing the items or products on offer, click on the item for further information and if interested in the purchase, can place an order by filling in an order form and clicking 'Submit', 'I Accept', or something similar.[6] These are called 'clickwrap' or 'webwrap' agreements. It is like taking the goods to the cash register in a shop, except that the cashier will usually be a computer instead of a person.[7] Contracts displayed on a website requiring a user to click a button to show acceptance, are generally non-negotiable and often are not read or viewed in their entirety before being accepted, raising the issue of whether there truly is mutual assent by the parties to the terms of the agreement.[8]

A third type of electronic contract is a 'shrinkwrap' agreement. A shrink-wrap agreement usually refers to a contract for a software product. It is commonly used in a software licence agreement. The terms and conditions in a shrinkwrap agreement are usually not visible until users start to install the software. In other words, the terms and conditions of the contract will be only available for review after the purchaser pays for the product. Currently, there are no consistent judicial opinions in the world on whether the terms and conditions of a shrinkwrap agreement that are not available before the conclusion of the contract of sales should be valid and enforceable. In the US, the Uniform Computer Information Transactions Act (UCITA) states that if the purchaser does not have an opportunity to review the terms before he pays, the product can be returned to the merchant.[9] However, the UCITA is not widely adopted in the US. In e-commerce practice it is advisable that the seller of software products makes the terms and conditions available for the purchaser to review prior to the placing of the order by displaying them directly on the website or providing a hyperlink.

Whatever the form of electronic contracting, trust is the basic element to foster transactions. In the process of an electronic trade, parties may not have met, or because of the fast speed of online transaction, parties may not have a chance to read terms and conditions of contracts precisely. There is a need to establish a certain level of trust which will, in return, build users' confidence in concluding electronic contracts.

At an international level, both the UNCITRAL Model Law on Electronic Commerce and the UN Convention employ the 'functional equivalent approach' with a view to determining how the purposes or functions of paper-based documents could be fulfilled through electronic commerce techniques.[10] In the EU, the EC Directive on Electronic Commerce contains three provisions[11] on electronic contracts, the most important of which is the obligation on Member States to ensure that their legal system allows for contracts to be concluded electronically. It can be found in Article 9(1), which in effect requires Member States to screen their national legislation to eliminate provisions which might hinder the electronic conclusion of contracts. Many Member States have introduced into their legislation a horizontal provision stipulating that contracts concluded by electronic means have the same legal validity as contracts concluded by more 'traditional' means. In

particular, as regards requirements in national law according to which contracts have to be concluded 'in writing', Member States' transposition legislation clearly states that electronic contracts fulfil such requirement.[12] In China, the National People's Congress adopted the new Contract Law which recognised electronic contracting in March 1999.[13] The new Contract Law of China (CLC)[14] implements several changes in contract formation rules. For example, a contract can now be made in any manner.[15] Under the CLC writings include agreement, letters, telegrams, telex, fax, electronic data information and electronic mail.[16]

3.3 The online contracting parties: who is contracting online?

In the scenario, who are the contracting parties? Are they seller A, buyer B or buyer B's computer? There is no provision governing this substantive issue under the UN Convention. Article 1 of the UN Convention sets the scope that it applies to 'parties whose places of business are in different states',[17] but 'neither the nationality of the parties nor the civil or commercial character of the parties or of the contract is taken into consideration'.[18] Thus, if A and B were contracting in different states ('but it is not necessary for both of those States to be contracting States of the UN Convention'), A and B would be contracting parties under the scope of the UN Convention.[19] Buyer B's computer cannot be regarded as a contracting party because it can't be considered a natural or legal person. The UN Convention does not directly have a ruling to contracting parties except for Article 4 referring to parties as 'originators and addressees'. Article 4(d) defines an 'originator' as 'a party by whom, or on whose behalf, the electronic communication has been sent or generated prior to storage, if any, but it does not include a party acting as an intermediary with respect to that electronic communication'. Article 4(e) determines 'addressee' as 'a party who is intended by the originator to receive the electronic communication, but does not include a party acting as an intermediary with respect to that electronic communication'. Thus, buyer B's computer should not be deemed to be a contracting party.

In the above scenario, how will it be possible to ascertain that the parties (buyer B and seller A) are really who they claim to be?

The word 'parties' is used in the UN Convention, which includes both natural persons and legal entities. The difference between recognising contracting parties online and offline is the method of identifying the parties. In the online environment, parties might never know and meet each other and there is no written signature in their e-contract.

The increased use of electronic authentication techniques as substitutes for handwritten signatures and other traditional authentication procedures has created a need for a specific legal framework to reduce uncertainty as to the legal effect that may result from the use of such modern techniques, namely electronic signatures.[20] The UN Convention does not attempt to identify specific technologies equivalent to particular functions of handwritten

signatures. Instead, it establishes general conditions under which electronic communications would be regarded as authenticated with sufficient credibility and would be enforceable in the face of signature requirements.[21]

At the same time, the UN Convention does not force parties to accept electronic communication, that is, the parties are free to decide whether or not to use electronic signatures.[22] The concept of 'party autonomy' is central to the UN Convention, in which Article 3 allows parties to exclude the application of the Convention as a whole or only to derogate from or vary the effect of any of its provisions. This important principle in contractual negotiations under the UN Convention is consistent with the view of UNCITRAL. Thus, no party should be compelled to use electronic means in the formation of contracts with regard to offers and acceptances.[23] The explanation given is that a party may lack access to electronic communication or the knowledge to use it or because of receipt or authentication problems. However, party autonomy does not allow the parties to relax statutory requirements on signatures in favour of methods of authentication that provide a lesser degree of reliability than electronic signatures, which is the minimum standard recognised by the UN Convention.[24]

For example, Article 9(3) of the UN Convention is intended to remove obstacles to the use of electronic signatures and does not affect other requirements for the validity of the electronic communication to which the electronic signature relates. According to Article 9(3)(a) of the UN Convention an electronic signature must be capable of identifying the signatory and indicating the signatory's intention in respect of the information contained in the electronic communication.

Article 9(3)(b) further establishes a flexible approach to the level of security to be achieved by the method of identification used under Article 9(3)(a). The method used under Article 9(3)(a) should be as reliable as is appropriate for the purpose for which the electronic communication is generated or communicated, in light of all the circumstances, including any relevant agreement.

There are two concerns in relation to Article 9(3): first, is it necessary to require the signatory's 'approval' of the information contained in the electronic communication, but not merely the indication of the party's intention? Does the notion of 'signature' necessarily imply a party's approval of the entire content of the communication to which the signature is attached? Second, how can one determine that the signature is 'as reliable as appropriate'? What is the 'reliability test'? However, these two obstacles are directly related to the implementation of electronic signature and authentication, which will be discussed in detail in Part III.

In the US, EU and China there are similar grounds as to the definition of online contracting parties as they provide rules on the identity requirements of valid electronic signatures. There are also differences among them. In the US, the Uniform Electronic Transactions Act (UETA) does not provide the definition of parties but an electronic agent, such as a computer program or other automated means, employed by a person. That person shall be

responsible for the results obtained by the use of that tool.[25] In China the China Electronic Signatures law explicitly clarifies that the person who provides electronic certification service shall be responsible for the service issuing a digital authentication certificate, although a digital certificate may be concluded by a natural person and an automated certification system.[26] In the EU there is an additional requirement related to the recognition of online contracting parties in the EC Directive on Electronic Commerce. Article 6(b) of the EC Directive on Electronic Commerce specifies the transparency requirements, and that commercial communications must be identifiable as such, and the natural or legal person on whose behalf the commercial communication is made must be identified.[27]

4 When is an electronic contract made?

When is an electronic contract concluded? Was it at the time when B completed the required web form, made a payment by debit card, or clicked the 'I agree' button to the terms and conditions? Could it be when A received B's order or when A amended the mistakes?

To answer the above questions it is necessary to examine the time of dispatch and receipt of an electronic communication, the rule relating to offer and acceptance and also errors in electronic communications.

4.1 Dispatch and receipt of an electronic communication

4.1.1 Time of dispatch

Different legal systems use various criteria to establish when a contract is formed and UNCITRAL favoured that it should not attempt to provide a rule on the time of contract formation that might be at variance with the rules on contract formation of the law applicable to any given contract.[1] The UN Convention on the Use of Electronic Communications in International Contracts (hereafter the UN Convention) offers guidance that allows for the application, in the context of electronic contracting, of the concepts traditionally used in international conventions and domestic law, such as 'dispatch' and 'receipt' of communications.[2]

The UN Convention redefines the dispatch and receipt of an electronic communication, which is different from the earlier legislation, UNCITRAL Model Law on Electronic Commerce. Article 10(1) of the UN Convention states that 'the time of dispatch of an electronic communication is the time when it leaves an information system under the control of the originator or of the party who sent it on behalf of the originator', whilst Article 15(1) of the UNCITRAL Model Law on Electronic Commerce, consistent with the UETA, defines it as 'the time of dispatch of an electronic communication is the time when it enters an information system outside of control of the originator or of the person who sent the data message on behalf of the originator'. The definition of 'dispatch' in the UN Convention is given as the time when an electronic communication left an information system under the control of

the originator, as distinct from the time when it entered another information system. It was chosen to mirror more closely the notion of 'dispatch' in a non-electronic environment.[3] The redefinition of the time of dispatch of an electronic communication is a welcome and timely change that better reflects the realities in today's technological environment.[4] However, the EC Directive on E-commerce lacks provisions defining 'the time of dispatch'.

The UN Convention is distinct from the rule of the Model Law on Electronic Commerce and UETA that the dispatch/sent of a data message occurs when it enters an information system outside the control of the originator/sender, or of the person who sent the data message on behalf of the originator/sender.[5] The UETA further provides a more precise explanation of 'an information system', namely that the information system can be designated or used by the recipient.

When applying the above rules to the earlier scenario the time of dispatch of electronic communications will occur when buyer B clicks the 'I agree' button to the terms and conditions and sends his order to seller A with the completed web payment form (i.e. giving credit card details), because when the action is done, buyer B is not in control of his order form any more and the order form enters an information system designated by seller A.

4.1.2 Time of receipt

As to the time of receipt, the EC Directive on Electronic Commerce (Article 11) stipulates that Member States shall apply the principle that: 'the order and acknowledgement of receipt are deemed to be received when the parties to whom they are addressed are able to access them'.

The EC Directive on Electronic Commerce is vague on what constitutes 'able to access'. It fails to explain the meaning of 'accessibility'.

The UN Convention (Article 9(2)) provides an objective criterion of 'accessibility', namely that 'Where the law requires that a communication or a contract should be in writing, or provides consequences for the absence of a writing, that requirement is met by an electronic communication if the information contained therein is accessible so as to be usable for subsequent reference'. The UN Convention Explanatory Note 2007 explains that the word 'accessible' implies that information in the form of computer data should be readable and interpretable,[6] and the word 'usable' is intended to cover both human use and computer processing.[7] Keeping receipt to a system accessible by the recipient removes the potential for a recipient leaving messages with a server or other service in order to avoid receipt.[8]

The UN Convention further analyses, in depth, that the time of receipt of an electronic communication is the time when it becomes capable of being retrieved by the addressee at an electronic address designated by the addressee.[9] It is presumed to occur when the electronic communication reaches the addressee's electronic address.[10]

This is comparable to Article 15(2) of the Model Law on Electronic

Commerce and §15(b) of the UETA. The difference is that the UETA provides further detail in that 'the electronic record is received when it is a form capable of being processed by that system'.[11] Another noticeable difference between the UN Convention and the Model Law on Electronic Commerce, as well as the UETA, is that the UN Convention does not mention the rules for receipt of electronic communications sent to a non-designated address.

However, none of them cover the issues as to how the sender proves the time of receipt, how the designation of an information system should be made, and whether the addressee could make a change after such a designation. There is also no explanation of what the meaning of 'capable of being retrieved' is, when the electronic communication is capable of being retrieved, or whether 'capable of being retrieved' is equivalent to 'able to access'.

Despite the difference in wording the effect of the rules on receipt of electronic communications in the UN Convention is consistent with the UNCITRAL Model Law on Electronic Commerce and the UETA. Article 10(2) of the UN Convention further regulates the rule on the time of receipt in the case where an electronic communication reaches the addressee's electronic address, which is presumed to be capable of being retrieved by the addressee at an electronic address designated by the addressee. In the author's opinion, this provision refers to three considerations in the determination of the time of receipt of an electronic communication as below:

- Firstly, accessibility should be defined under the designated address. For example, if A sends B an offer at his home email address which is rarely used for business purposes, it may not be deemed received if B designated his official business email address as the sole address for business purposes. Thus, even though the email is accessible at B's home address, it will not constitute receipt of the electronic communication.
- Secondly, the retrievability should be distinct from the accessibility. That the electronic communication is accessible does not constitute the presumption that the electronic communication is retrieved. The rationale is that if the originator chooses to ignore the addressee's instructions and sends the electronic communication to an information system other than the designated system, it would not be reasonable to consider the communication as having been delivered to the addressee until the addressee has actually retrieved it.[12]
- Thirdly, receipt of an electronic communication at a non-designated electronic address should fulfil two conditions: retrievability and awareness. In other words, receipt at a non-designated electronic address occurs when (a) the electronic communication becomes capable of being retrieved by the addressee and (b) the addressee actually becomes aware that the communication was sent to that particular address.

In addition, the final noteworthy difference is that the EC Directive on Electronic Commerce only covers the acknowledgement of receipt of

electronic communications, whereas the Model Law on Electronic Commerce and UETA include the acknowledgement of all electronic records.[13] The scope of the UN Convention is even wider as it embodies all electronic communications which are made by means of data messages.[14]

4.2 Offer and acceptance[15]

4.2.1 International legislative developments

At the international level, conventions and model laws governing electronic commercial transactions do not include a substantial rule on the effectiveness of offer and acceptance for the purposes of contract formation. The non-cyber-specific international instrument, the United Nations Convention on Contracts for the International Sale of Goods (CISG), provides provisions on the rules of offer and acceptance. For example, Article 15(1) of the CISG specifies that '[a]n offer becomes effective when it reaches the offeree'. The Advisory Council stated that for purposes of this provision, '[t]he term "reaches" corresponds to the point in time when an electronic communication has entered the offeree's server'.[16] Article 18(2) of the CISG further provides that:

> an acceptance of an offer becomes effective at the moment the indication of assent reaches the offeror. An acceptance is not effective if the indication of assent does not reach the offeror within the time he has fixed or, if no time is fixed, within a reasonable time, due account being taken of the circumstances of the transaction, including the rapidity of the means of communication employed by the offeror. An oral offer must be accepted immediately unless the circumstances indicate otherwise.

The Advisory Council noted for purposes of this provision: an acceptance becomes effective when an electronic indication of assent has entered the offeror's server, provided that the offeror has consented, expressly or impliedly, to receiving electronic communications of that type, in that format, and to that address.[17]

It is obvious that the CISG adopts the acceptance rule in determining a valid offer and acceptance in paper-based contracts. It is also notable that the Advisory Council of the CISG applies the same rule to the acknowledgement of a valid electronic offer and acceptance by simply interpreting 'reach offeree or offeror' as 'enter the offeree's or offeror's server' without any clear clarification of the time of dispatch or receipt of an electronic communication. The UN Convention on the Use of Electronic Communications in International Contracts (hereafter the UN Convention) does not provide a provision on the validity of offer and acceptance, but includes a clear rule on the time and place of dispatch and receipt of electronic communications. It is

still debatable whether the UN Convention should propose a provision on when an offer and acceptance in electronic communications takes effect, and whether the existing rule of the time of dispatch and receipt of electronic communications will be sufficient to ascertain an offer and acceptance. If so, how should it be explained, and if not, what should be done about it?

Whether a contract has been formed is one of the most critical questions concerning internet transactions. An English case, which is famous as a starting point for the law in this area for further reference in other countries, is *Entores v Miles Far East Corp*.[18] The leading judgment in the Court of Appeal was given by Lord Denning:

> His approach was to take as his starting point a very simple form of communication over a distance, that is, two people making a contract by shouting across a river. In this situation, he argued, there would be no contract unless and until the acceptance was heard by the offeror. If, for example, an aeroplane flew overhead just as the acceptor was shouting his agreement, so that the offeror could not hear what was being said, there would be no contract. The acceptor would be expected to repeat the acceptance once the noise from the aeroplane had diminished. Taking this as his starting point, he argued by analogy, that the same approach should apply to all contracts made by means of communication which are instantaneous or virtually instantaneous.[19]

The case shows that when the means of communication being used by parties is almost instantaneous the acceptance rule should prevail over the postal rule. The House of Lords further approved this decision in *Brinkibon Ltd v Stahag Stahl und Stahlwarenhandelsgesellschaft mbH*.[20] On this basis, regarding emails or clickwrap contracts as falling into the 'instantaneous' category, the acceptance should take place where it was received, rather than where it was sent. However, an email may not be opened as soon as it arrives, and it may be not read until some time after it has been delivered. Thus, it is crucial to determine the time that the acceptance takes effect. It is suggested that the contract will be formed, at the earliest, when the acceptance is received by the offeror's email system and is available to be read. At the latest, it should be regarded as complete after the passing of a reasonable period of time for the acceptance to have been read as expected.[21] With regard to a web agreement, the contract would be made where the offeror had acknowledged to the offeree that his or her offer was accepted, either by means of a direct response on the website or by a subsequent email, which is called the 'information duty'.

The online contract cannot be binding on the parties until there has been an agreement. The normal analytical tool used to test such a meeting of minds is that of offer and acceptance. Generally, a binding commitment emerges when the offeror has knowledge of the acceptance and when the offeree is similarly apprised of this. However, the rules on offer and acceptance reflect cultural, economic and political ideas about consensual activity.

According to contract law a promise with consideration is deemed to bind the parties when an offer is accepted.[22]

The process of contract negotiation over the internet is the same as in physical reality: invitation to treat, offer and counter-offer, and final acceptance. The distinction between an invitation to treat and an offer is that an invitation to treat is not binding, whilst an offer, met with acceptance, may form a contract. The distinction does not entitle a website to induce a customer to enter a contract by using misleading statements. If a factual statement prior to a contract being formed is classified as misleading, the induced party may be entitled to claim damages, rescind the contract, or even both.[23]

The UN Convention is silent on the validity of offer and acceptance, except for 'invitation to make offer'.[24] It defines 'invitation to make offer' as a proposal to conclude a contract, which is generally accessible to parties making use of information systems, rather than addressed to one or more specific individuals. It is similar to the concept of 'an invitation to treat' in the traditional law of paper-based contract. Displaying information of products including price, quantity and delivery method is an invitation to make offer rather than a real offer as the information on the website is available to the public but not to one or more specific persons. This is evidenced by an English leading case *Pharmaceutical Society of GB v Boots Cash Chemists*.[25] The Court of Appeal held that the display of products on the shelves was not an offer, but an invitation to negotiate. Boots did not infringe the Pharmacy and Poisons Act 1933 as the sale of products took place at the cash desk. It was the customer that made the offer to buy the goods by putting the goods into the basket. It is up to the pharmacist to accept or reject the offer at the cash desk.

The difficulty that may arise in this context is how to strike a balance between a trader's possible intention (or lack thereof) to be bound by an offer, on one hand, and the protection of relying on parties acting in good faith, on the other hand.[26] The general principle that offers of goods or services that are accessible to an unlimited number of persons are not binding applies even when the offer is supported by an interactive application.[27] Typically, an 'interactive application' is a combination of software and hardware for conveying offers of goods and services in a manner that allows for the parties to exchange information in a structured form with a view to concluding a contract automatically.[28] Article 11 of the UN Convention is not intended to create special rules for contract formation in electronic commerce. Accordingly, a party's intention to be bound would not suffice to constitute an offer in an absence of those other elements, such as the quantity and price of the goods.[29] But what will happen if the buyer orders a large quantity of goods that the seller may not be able to supply?

In traditional contract cases there are evidences of protection of sellers. For example, in the case of *Grainger & Son v Gough*,[30] the judge held that the transmission of price lists did not amount to an offer to supply an unlimited quantity of products described at the price named, as the stock of products from advertisers or merchants could be limited. The House of Lords further

approved this decision in *Esso Petroleum Ltd v Customs and Excise Commissioners*.[31] Without reasonable expectations advertisers or merchants could have been in breach of contractual obligations when they failed to supply a large order. In e-commerce practice it is common that e-retailers will indicate the estimated quantity of products that are available for sale on the website, whereas, in the international trade industry, the companies or manufacturers may clarify the possible length of production per unit or container shipment.

EU legislative status

In the EU the EC Directive on Electronic Commerce is also silent on the effectiveness of offer and acceptance, but it obliges offerees to acknowledge the receipt of an offer (order) 'without undue delay and by electronic means'.[32] The supplier is entitled first to acknowledge receipt of the offer, and then to accept the offer, according to the rule of 'time of acceptance'.[33]

US legislative trends

In the US, with regard to the efficiency of offer and acceptance, there is only the UCITA, which provides that 'a contract may be formed in any manner sufficient to show agreement, including offer and acceptance or conduct of both parties or operation of electronic agents which recognizes the existence of a contract'.[34] It also specifies that, in the case of a computer information transaction, 'a contract is formed when an electronic acceptance is received'.[35] The UETA and ESIGN Act are silent on the appropriate rule for the timing of an acceptance.[36] However, §14 of UETA validates transactions formed between parties by the interaction of their electronic agents even if they were not aware of the resulting terms or agreements. The section also validates the formation of contracts by interactions between an electronic agent and an individual who voluntarily performs actions with knowledge or reason to know that they will cause the electronic agent to complete performance. The ESIGN Act, whilst generally validating the use of electronic agents,[37] does not address these issues. UETA, §15 provides that a record is 'sent' when it is properly addressed in a form capable of being processed and it enters a system outside that of a sender or system to which the addressee has access, and that a record is 'received' when it enters a system designated for receipt of such information in a form capable of being processed. Although the parties may contractually alter this rule it provides a bright-line default rule. The ESIGN Act is silent on this issue.[38]

The UCITA validates electronic contracts by replacing the concept of a 'writing' with that of a 'record', stating that contracts valued at $5,000 or more are not enforceable unless 'the party against which enforcement is sought authenticated a record sufficient to indicate that a contract has been formed and which reasonably identifies the copy or subject matter to which the contract refers'.[39] The UETA also imposes a record requirement rather

than a writing requirement. Both UCITA and UETA define a 'record' as 'information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form' and an 'electronic record' as a record that is created, generated, sent, communicated, received, or stored by electronic means.[40] Therefore, both UCITA and UETA broaden the traditional common law writing requirement and clarify the validity and enforceability of certain electronic contracts.

Chinese legislative framework

In China, the Contract Law of China (CLC) states that parties may conclude their contract by way of offer and acceptance.[41] Under the CLC the common law postal rule does not apply. An acceptance is effective at the time when the offeree indicates assent, and it should reach the offeror within the time fixed in the offer.[42] If there is no fixed time in the offer, the offer is deemed to be effective within a reasonable time. Compared with the United Nations Convention on Contracts for the International Sale of Goods, 1980 (CISG) the offer and acceptance rules of the CLC are similar.[43] In contrast to the CLC, the China Electronic Signatures Law does not directly regulate the rules of offer and acceptance of electronic contracts. However, Articles 9 to 12 deal with the sending and receipt of data messages. Article 10 states that if the receiving of any data message needs to be confirmed as prescribed by laws and administrative regulations or the stipulations of the parties, the receipt shall be acknowledged. Article 11 deals with the time the data message is deemed to be sent and received. It states that the time when any data message enters into a certain information system out of the control of the addresser shall be regarded as the time for sending the data message. It further states that where a recipient has designated a specific system to the sender for sending the data message the time at which the data message enters such a system shall be deemed to be the time of the receipt of the data message. If no given system is designated, the time when the data message enters into any system of the recipients for the first time shall be regarded as the time for receiving the data message.

Can the postal rule apply to E-contracting?

Traditionally, English courts have been in favour of the postal rule because the court felt that the acceptance rule might result in each side waiting for confirmation of receipt of the last communication ad infinitum.[44] This would not promote business efficacy. Therefore, in order to promote business efficacy, it would be much better if, as soon as the letter of acceptance was posted, the offeree could proceed on the basis that a contract had been made and take action accordingly.[45] In the court's view the conduct of business will in general be better served by giving the offeree *certainty*.[46] In *Household Fire and Carriage Accident Insurance Co v Grant*,[47] it was held that even if an

acceptance was lost and it never arrived at its destination the contract was still concluded. This is still the rule under English contract law. However, the postal rule itself has limitations. It only applies to acceptance, and not to any other type of communication such as offer or counter-offer.[48] Communication of the offer is required in virtually all situations as the person to whom the offer is addressed must be aware of it.[49] In short, the postal rule was created to provide certainty in contractual formation at a time when the communication system involved unavoidable delays, because the postal stamp enables us to determine easily the time of posting an acceptance.

On the other hand, the postal rule also contains two major disadvantages: firstly, the offeror will not be aware of the contract until a few days after the letter of acceptance was posted by the offeree; secondly, the acceptance letter might never be received by the offeror, because it might be lost by the post office. This failure of delivery would prevent the offeror from knowing that a contract had been made.

As noted above, the postal rule states that if the offeree contemplates acceptance by post the acceptance is effective once posted rather than when it is received. It provides the offeree with confidence that an acceptance once posted will be effective, even if the postal system delays delivery of the acceptance beyond the offer date.[50] That is, the contract is deemed to have been concluded at the moment the acceptance is placed into the postal system.[51] The impact of the traditional postal rule on the offer and acceptance process in electronic contracting must be assessed.

In the era of information technology, accepting an offer can be through electronic means and there are some similarities between email and post. For instance, dispatching an email is identical to dropping a letter in a red post box. Just like for the sender of a letter, the sender of an email will have no control over it after having pressed the send button, as it will be transmitted to his internet service provider (ISP).

However, an issue which arises when parties are communicating by electronic means is whether an offer can be revoked, or if the offeree can reject an offer once an acceptance has been sent and when it is received.[52] Some scholars like Professor Murray, Professor Walker and Professor Gloag argue that email and clickwrap agreements are different and have to be treated in a different way. They proposed that the postal rule should apply to emails, whilst clickwrap agreements should employ the acceptance rule. In my view, although emails and clickwrap agreements are different, they have something in common in that they deliver messages much faster than normal postal mail.

Postal mail services v. electronic mail services

Compared to postal mail services, electronic communications have three major differences in character:

- Firstly, although email is not completely instantaneous, it is, unlike

postal mail, normally very quick. Sometimes there are delays, but it is rare and it normally lasts less than a day. Thus, the postal rule loses its traditional function of efficiency in email communications.

- Secondly, current software technology makes it possible not only to determine exactly when the acceptance email was sent by the offeree, but also when it was received by the offeror's server. Hence, contractual certainty will be established by proof of receipt.
- Thirdly, another point to take into account, which makes email communications different from postal ones, is that when the acceptance is sent to the offeror, if no direct reply follows, under the current software system an automated message with three possible responses may be sent to the offeree: that 1) the message has been received or delivered; that 2) the message has been read; or that 3) the message failed to be delivered. However, the speed at which the packages of information are forwarded along the different routes before they are reassembled at their final destination is more dependent on the workload of the servers and networks they use than the geographical distance of the computers. It may therefore be possible to receive a 'return to sender' message in your inbox a few days later.[53] Thus, when the email was sent, it might have never reached the recipients due to technical failures or some other possibilities. There will be a delay between the sending of an acceptance and its coming to the attention of the offeror.

The receipt acknowledgement of email, such as 'your message has been received or delivered', performs on this occasion similar functions as 'recorded delivery' mail, creating again an element of certainty. This will have, unlike the postal rule, the advantage of enabling both parties to know that there is a contract. Thus, taking account of the above features of email, the acceptance rule should prevail over the traditional postal rule in the electronic communication environment. That is, the acceptance takes effect when it reaches the offeror.

Solution: the application of the acceptance rule

Due to the characteristics of electronic communications, it would be convenient and harmonious to apply the acceptance rule to electronic transactions. English courts have already accepted that the postal rule should not be applied where it would lead to 'manifest inconvenience or absurdity'.[54] This position is also supported in the US Restatement (Second) of Contracts, which provides that acceptance given by telephone or other medium of substantially instantaneous two-way communication is governed by the principles applicable to acceptance where the parties are in the presence of each other.[55] Thus, the acceptance rule – that the acceptance becomes effective when it reaches the offeror – should be applied in electronic contracting, especially clickwrap agreements because it is as instantaneous as

face-to-face or oral interactions. The question then arises as to whether we should apply the same rule, 'the acceptance rule', to email as to clickwrap agreements.

If the acceptance rule is applied, then another issue must be answered: 'Is there a contract when the acceptance is received by the server or when it is actually received and read by the offeror?'[56]

There are three possibilities applying the acceptance rule in electronic mail communications:

- firstly, at the earliest stage, the contract is concluded when the acceptance is received by the offeror and it is available to be read;
- secondly, at the middle stage, the contract will be formed when the acceptance is received by the offeror and is assumed to be read by him within a reasonable time;
- thirdly, at the latest stage, the contract will be established when the acceptance is received and actually read by the offeror.

In relation to clickwrap agreements the contract will be formed when the acceptance has been received by the offeror's server. The server then automatically responds to it with an acknowledgement of receipt.

As the outcomes above show, there is a crossing point between email contracting and clickwrap agreements, that is, the acceptance must be received and the corresponding acknowledgement must follow. Therefore, we could treat email and clickwrap agreements as the same standard of electronic communications in contracts. Meanwhile, in order to be compatible with the determination of 'the time of receipt of electronic communications'[57] in the UN Convention, the uniform rule should be that an electronic contract will be concluded when the acceptance is received and has been retrieved or read by the offeror within a reasonable time. This would be presumed with the evidential automatic message confirming that 'the message has been received', 'the message has been delivered' or 'the message has been read'. In the author's view, an extra explanatory note or an amendment (addition) clause of the effectiveness of the electronic offer and acceptance in the UN Convention is a necessity to remove the legal uncertainty of the valid process of electronic contracting and boost users' confidence in doing business online.

Looking back on the above scenario, Party A's advertisement on his website should be deemed to be an invitation to treat, because it does not specifically target Party B, but it is instead open to any Party X. When B completes the order form and agrees to the standard terms and conditions A's invitation to treat becomes a firm offer. When B clicks the button to dispatch his order form, it should be regarded as an acceptance to A's offer. The complicated issue raised here is whether B can amend the offer after the acceptance has been received and read; this will be discussed further under the section of errors in electronic communications.

4.3 Availability of contract terms

In contract law terms become parts of contracts because the parties agree to them. In electronic contracting parties agree to the terms and conditions (T&C) which are a record of data messages appearing on the PC screen. Sometimes, after clicking the 'I agree' button, T&C disappear and it is impossible to get back to them or download them afterwards. Even if it is possible to access them or reproduce them afterwards often standard T&C are inalterable and parties asked to 'agree' to the terms in some instances will have no easy alternative other than to submit.[58]

In response to the above concerns some legislation requires that the T&C should be available to be downloaded or reprinted afterwards, which aims to enhance legal certainty, transparency and predictability in international transactions concluded by electronic means.[59] However, some legislation is silent on the consequences of the failure to comply with requirements of availability of T&C electronically.

Article 10(1)(b) of the EC Directive on Electronic Commerce requires that the concluded contract should be filed by the service providers, and it must be accessible. Furthermore, Article 10(3) states that 'contract terms and general conditions provided to the recipient must be made available in a way that allows him to store and reproduce them'. The EC Directive on Electronic Commerce does not provide the solution for determining the consequences of a failure to provide the stipulated information.

The UN Convention on the Use of Electronic Communications in International Contracts (hereafter the UN Convention) does not impose any requirement for contracting parties to make available the contractual terms in any particular manner nor give any consequence for failure to perform the duty. Article 13 of the UN Convention preserves the application of domestic law that may require a party to make available to the other party the electronic communications containing the contractual terms.[60] Because there is a wide variety of consequences for failure to make the T&C available subject to domestic laws, for example, some might suggest that failure to make the T&C available should constitute an administrative offence and incur a fine, whereas some might give the customer the right to seek an order from the court to enforce the requirement of making the T&C available, or the contract does not enter into force until the time when the merchant has complied with its obligations.[61] However, usually the rule of imposing a duty of making the T&C available and its consequence of failure to do so does not exist in paper-based offline transactions; therefore international commercial contract legislation did not create any sanctions.[62] It should be left to competition laws or consumer laws to deal with.[63]

In the author's opinion, electronic communications are fundamentally different from paper-based communications. Electronic evidence is crucial for any possible disputes that might arise later. It is necessary to regulate the rule of the availability of T&C in an international instrument such as the UN

Convention and the issue of making the T&C available should be compulsory, whether by means of displaying on the website, downloading from the network, or requesting from merchants, simply because the rule of consent is the kind of knowledge that national legal systems require from business partners in order to infer their (explicit or implied) consent on T&C. The principle of mutual consent rules on contract formation in the majority of countries requires the modification of T&C to be notified and accepted by counter-parties in order to become part of the contract. Regarding the issue of when such knowledge of T&C shall be gained, the majority of countries require prior knowledge or knowledge at least at the time of contract conclusion[64] of the receipt of the contract or agreement, while the other view is that an e-market participant shall in principle be bound by T&C if, at the time of agreement, it was aware or should have been aware of such terms using ordinary care.[65] Thus, the requirements of the availability of contract terms will fulfil the requirements of the awareness of the contract or sale agreement. If the availability of contract terms is guaranteed in electronic contracting it will be much more efficient and convenient than offline contracting. For example, when a wholesaler goes to Acme wholesale store to order products and pays for them at the till, how often will they check the T&C on the back of the receipt? Alternatively, if a wholesaler purchased products through Acme's website where the negotiation tool of the T&C was provided, it might be more likely that the wholesaler would read and select the T&C. Thus, T&C in online circumstances might prevail over T&C in the offline world.

However, there is no need to have a specific provision governing the consequences of failure to do so under the UN Convention, because it relates to substantive laws, which lead to different outcomes and are too different to be uniformed. Thus, it should be dealt with according to domestic laws.

4.4 Error in electronic communications

Mistake means that parties make errors in subject matters or the terms of the contract as to quality or quantity etc. Misrepresentation refers to a false statement of fact that induces the other party to enter into a contract. In traditional contract laws mistakes can make a contract void whilst misrepresentation can make a contract voidable. Mistakes that constitute a void contract should be fundamental.[66] In the case of *Seatbooker Sales Limited v Southend United Football Club*, the original contract of internet ticket sales service was valid as no mistake and misrepresentation were found.[67] In the author's view, error in electronic communications should include both electronic input mistakes and electronic false statement. The concepts of mistakes and misrepresentation in electronic contracts should be the same as those in offline contracts.

One feature that distinguishes online methods of communication from traditional media is that software now assumes an instrumental role in

constituting agreements. If the buyer intends to make a purchase online he will need to engage with the input data. The software interprets the steps automatically in the negotiations purely on the basis of the clicks made by the buyer. If the buyer does not communicate the range of predicted responses, either the process will cease or a new range of options will be presented for consideration.[68] Thus, there are differences in the process of forming a contract electronically and those that are paper-based.

Is 'error in electronic communications' equivalent to 'the traditional mistake and misrepresentation in contracts'? If not, what are the differences?

In answering that question, one should ask whether there is something more we need to protect errors in electronic contracting beyond the existing contract law.

4.4.1 Current legislation in electronic errors

International approach

Article 14 of the UN Convention details the rules of error in electronic communications as:

1. Where a natural person makes an input error in an electronic communication exchanged with the automated message system of another party and the automated message system does not provide the person with an opportunity to correct the error, that person, or the party on whose behalf that person was acting, has the right to withdraw the portion of the electronic communication in which the input error was made if:
   (a) The person, or the party on whose behalf that person was acting, notifies the other party of the error as soon as possible after having learned of the error and indicates that he or she made an error in the electronic communication; and
   (b) The person, or the party on whose behalf that person was acting, has not used or received any material benefit or value from the goods or services, if any, received from the other party.
2. Nothing in this article affects the application of any rule of law that may govern the consequences of any error other than as provided for in paragraph 1.

According to Article 14(1) of the UN Convention there are four conditions on withdrawing the portion of electronic communications in which input error was made.

Firstly, Article 14 of the UN Convention applies to a very specific situation that is only concerned with errors that occur in transmissions between a natural person and an automated message system when the system does not

provide the person with the possibility to correct the error.[69] Secondly, the UN Convention further authorises a party who makes an error to withdraw the portion of the electronic communication where the error was made under the conditions of '(a) notifying the other party of the error as soon as possible after having learnt of it, and (b) not having used or received any material benefit or value from the goods or services'.[70]

EU approach

Compared with the UN Convention the EC Directive on Electronic Commerce is much simpler in regulating input errors. It mainly requires the service provider to provide information and make technical means available, appropriate, effective and accessible prior to the placing of the order.

The EC Directive on Electronic Commerce obliges websites to provide in a clear, comprehensible and unambiguous manner information about how customers may identify and correct input errors before they place an order.[71] For instance, the EC Directive on Electronic Commerce requires certain procedural information before parties can enter into a contract. To avoid technical problems or mistakes by the contracting parties the service provider must provide the following information:[72]

- the different technical steps that are to be followed to conclude the contract;
- whether the contract will be filed by the service provider and whether it will be accessible;
- the technical means for identifying and correcting input errors prior to the placing of the order; and
- the languages offered for the conclusion of the contract.

Furthermore, Article 11(2) of the EC Directive on Electronic Commerce provides that 'Member states shall ensure that, except when otherwise agreed by parties who are not consumers, the service provider makes available to the recipient of the service appropriate, effective and accessible technical means allowing him to identify and correct input errors, prior to the placing of the order'.

US approach

The Second Restatement of Contracts, §153 states:

> Where a mistake of one party at the time a contract was made as to a basic assumption on which he made the contract has a material effect on the agreed exchange of performances that is adverse to him, the contract is voidable by him if he does not bear the risk of the mistake under the rule stated in §154, and (a) the effect of the mistake is such

that enforcement of the contract would be unconscionable, or (b) the other party had reason to know of the mistake or his fault caused the mistake.

The Uniform Electronic Transactions Act (UETA), §10 regulates the effect of change or error. It states that if a change or error in an electronic record occurs in a transmission between parties to a transaction, the following rules apply:

(1) If the parties have agreed to use a security procedure to detect changes or errors and one party has conformed to the procedure, but the other party has not, and the nonconforming party would have detected the change or error had that party also conformed, the conforming party may avoid the effect of the changed or erroneous electronic record.
(2) In an automated transaction involving an individual, the individual may avoid the effect of an electronic record that resulted from an error made by the individual in dealing with the electronic agent of another person if the electronic agent did not provide an opportunity for the prevention or correction of the error and, at the time the individual learns of the error, the individual:
    (A) promptly notifies the other person of the error and that the individual did not intend to be bound by the electronic record received by the other person;
    (B) takes reasonable steps, including steps that conform to the other person's reasonable instructions, to return to the other person or, if instructed by the other person, to destroy the consideration received, if any, as a result of the erroneous electronic record; and
    (C) has not used or received any benefit or value from the consideration, if any, received from the other person.
(3) If neither paragraph (1) nor paragraph (2) applies, the change or error has the effect provided by other law, including the law of mistake, and the parties' contract, if any.
(4) Paragraphs (2) and (3) may not be varied by agreement.

As outlined in the US Second Restatement and UETA, the conditions of withdrawal of error in electronic communications in the US are similar to those of the UN Convention. However, there are still some differences. For example, §10(1) of the UETA does not define the scope of 'between parties', in other words, it is not clear whether the parties of the error communication can be natural persons or, like the UN Convention, the error communication should occur between a natural person and an automated transactions system.

The rule of error input in the UETA is for both B2B and B2C transactions, whereas §214 of the Uniform Computer Information Transactions Act (UCITA) governs electronic error, only for consumer defences. It specifies that:

> (a) In this section, 'electronic error' means an error in an electronic message created by a consumer using an information processing system if a reasonable method to detect and correct or avoid the error was not provided.
> (b) In an automated transaction, a consumer is not bound by an electronic message that the consumer did not intend and which was caused by an electronic error, if the consumer:
>
> (1) promptly on learning of the error:
> (A) notifies the other party of the error; and
> (B) causes delivery to the other party or, pursuant to reasonable instructions received from the other party, delivers to another person or destroys all copies of the information; and
> (2) has not used, or received any benefit or value from, the information or caused the information or benefit to be made available to a third party.
>
> (c) If subsection (b) does not apply, the effect of an electronic error is determined by other law.

As provided above, both UETA and UCITA apply to the situation that is 'in an automated transaction'. They are common in that they both impose the duty of prompt notification of the error, the requirement of taking reasonable steps accordingly and the condition of non-use of, or non-benefit from, the goods.

Chinese approach

There is no provision of error in electronic communications under the China Electronic Signatures Law. In the absence of particularised legislation errors occurring over the internet in China shall be subject to the Contract Law of the People's Republic of China adopted in 1999. According to Article 54 of the Contract Law of China:

> a party shall have the right to request the people's court or an arbitration institution to modify or revoke the following contracts:
>
> (1) those concluded as a result of significant misconception;
> (2) those that are obviously unfair at the time when concluding the contract.
>
> If a contract is concluded by one party against the other party's true

> intentions through the use of fraud, coercion, or exploitation of the other party's unfavourable position, the injured party shall have the right to request the people's court or an arbitration institution to modify or revoke it.[73]

In the Contract Law of China the terms 'misconception', 'unfair', 'fraud', and 'exploitation' have been introduced to determine the validity of a contract and the legality of modification or revocation of the contract. Such terms are equivalent to mistake and misrepresentation in common law.

4.4.2 Obstacles in regulating electronic errors

Pricing errors often appear on e-commerce websites. For example, when Amazon's UK site advertised iPaq Pocket PCs for £7.32 instead of the normal price of £300 thousands of orders were placed, with some people buying 50 or more.[74] In the US, United Airlines wrongly posted a San Francisco to Paris flight for £24.98. Also, in 2003 Amazon.com wrongly listed the price of television sets at $99.99 instead of $1049 each and received 6,000 orders.

Mistakes occur easily on the internet when users input data because of the automated and speedy features of the internet. Misrepresentation also occurs easily with online shopping as products cannot be actually seen, touched and tested by buyers. When disputes happen online buyers usually find it difficult to prove mistake and misrepresentation.

There are four major concerns about electronic mistakes and misrepresentation in expression: first, who should be responsible for the mistake and misrepresentation? How should the balance be kept between the interest of a mistaken party not to be bound by unintended expressions of promises and the interest of a party relying on a promise to be able to act upon it? Second, how can one know whether it was a mistake or a misrepresentation and not merely a change of mind? Third, what will be the reasonable time bar for mistake or misrepresentation to be discovered and informed? Fourth, what are the conditions for withdrawal or avoidance of electronic communications affected by errors?

Two of the main features of electronic communication are its speed and automation. Both of these features increase the risks of making mistakes that cannot be easily corrected before they reach the addressee and before the addressee takes action in reliance on the mistake.[75] For example, you offered your business partner $20 per product A by email, but immediately realised that the price had increased in line with inflation; thus you sent another email to inform your business partner that the price had to change to $28 per product A. So will this constitute a valid new offer?

In traditional contract law once the offer is accepted the contract is formed. In the electronic environment, the offer may be amended if the person, or the party on whose behalf that person was acting, notifies the other party of the error as soon as possible after having learned of the error and indicates

that he or she made an error in electronic communication.[76] This presumption is based on two conditions: one is the timing – 'notifying the other party as soon as possible', and the other is the indication of the error in electronic communication.

These conditions have the effect of limiting the time within which an electronic communication can be withdrawn pursuant to Article 14 of the UN Convention. Under Article 14(1) the right of withdrawal is only available if the notification of the input error is made 'as soon as possible' after the party had learnt of the error, and the party 'has not used or received any material benefit or value from the goods or services' received.[77] A question arises as to the effect of a withdrawal made pursuant to Article 14. For example, where the erroneous communication formed part of an offer and the automated message system of the other party accepted that offer prior to receiving notice of the withdrawal; under the normal rules of contract formation, a contract would have been formed upon the acceptance. If the withdrawn portion contained some essential term of the contract, what would be the effect of the withdrawal?

There are two possible effects of the withdrawal. Firstly, the effect of a withdrawal of the erroneous portion could be that the electronic communication is to be regarded as never having contained that erroneous portion. Secondly, the effect of the withdrawal of the erroneous portion could be that the electronic communication is to be regarded as having been sent with the erroneous portion, which portion was subsequently withdrawn.[78] During the preparation of the UN Convention, it was argued that the remedy should be limited to the correction of an input error, so as to reduce the risk that a party would allege an error as an excuse to withdraw from an unfavourable contract.[79]

In the author's view 'withdrawal' should be included to protect the right of the party when the party has unintentionally hit a wrong key or web button and sent a message that he did not intend to send. In the online environment, recall or replacement of an error message can sometimes be easier and quicker than in an offline situation.

4.4.3 Solution I: implication from the Microsoft Outlook case

There is an interesting functional tool 'recall or replace a message you've already sent'[80] in Microsoft Outlook software which might also reveal some trends on the conditions of withdrawal or amendment of errors in electronic communications.

To recall or replace an error message online can be easier and quicker than in an offline situation. If you use a Microsoft Exchange Server email account you can recall or replace a message if its recipient is logged on and using Microsoft Outlook and has not read the message or moved it from their inbox. The author's concern is whether 'recall or replace a message' function can comply with the rule of 'error in electronic communications'.

Before answering it, let's look at the Microsoft Message Tool:

Figure 4.1

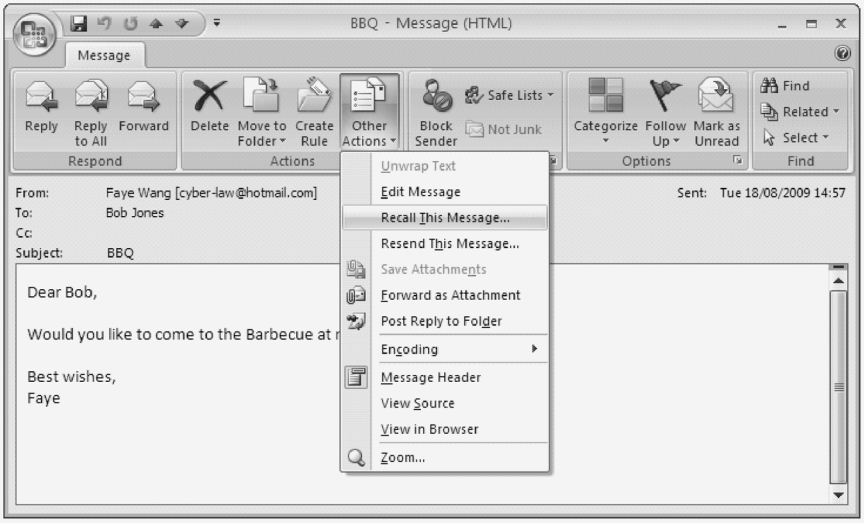

Figure 4.2

According to the above model, the method is:

1) In Mail, in the Navigation Pane, click Sent Items.
2) Open the message you want to recall or replace.
3) In the message window, on the Actions menu, click Recall This Message.

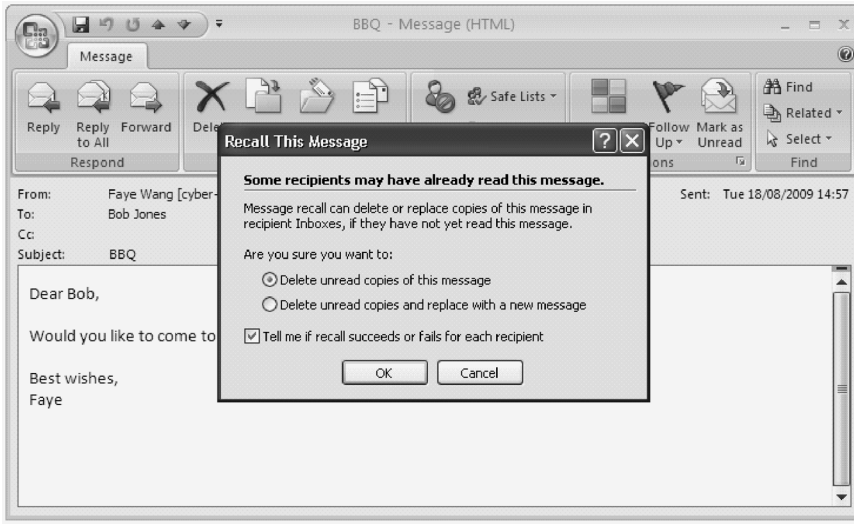

Figure 4.3

Next, do one of the following:

1) Recall the message: Click 'Delete' unread copies of this message and select the 'Tell me if recall succeeds or fails' for each recipient check box if you want to be notified about the success of the recall or replacement for each recipient.
2) Replace the message: Click 'Delete' unread copies and replace with a new message, select the 'Tell me if recall succeeds or fails' for each recipient check box if you want to be notified about the success of the recall or replacement for each recipient, click 'OK', and then type a new message. To replace a message, you must send a new one. If you do not send the new item, the original message is still recalled.[81]

There are two drawbacks to the above function of recall and replacement: first, this technique is limited because the feature can only be used if your emails are handled by a Microsoft Exchange Server, which is a server that picks up the emails for the whole company and then passes them to the right client, so you can't use this feature with your home PC which connects to your email provider directly. Second, the technique is inconsistent with one of the conditions of the rationale behind the error in electronic communications under the UN Convention. Microsoft Outlook requires that a message can be recalled or replaced if its recipient has not read the message or moved it from their inbox without any time limit, whereas the UN Convention sets the restriction that the person or the representative should notify the other party of the error as soon as possible after having learned

of the error, although the UN Convention does not define what 'as soon as possible' is.

In the absence of the time restriction of the message recall mechanism on Microsoft Outlook the principle of 'the intentions of the parties' regarding correction of input data should be deemed to be a criterion in determining whether the recalling or replacing of a message is done in good faith, as indicated by a leading case *Brinkibon Ltd v Stahag Stahl und Stahlwarenhandel GmbH*. It states:

> Some error or default at the recipient's end which prevents receipt at the time contemplated and believed in by the sender. No universal rule can cover all such cases; they must be resolved by reference to the intentions of the parties, by sound business practice and in some cases a judgment where the risks should lie.[82]

In addition, there are two possible legal effects in recalling and replacing an email: first, it would mean that, for example, an offer containing an error in the quantity of goods would be regarded as an offer which never contained any quantity of goods at all. Such an offer would probably not give rise to a valid contract. Second, if the same offer containing the error in the quantity of goods was already accepted, and the erroneous portion was subsequently withdrawn, it would raise a question as to the effect of such a withdrawal on a concluded contract.[83] For example, if a person mistakenly typed 14 when he intended to order just 4 items, the order will not be corrected so as to take effect as an order for 4 items. Under the former scenario, he will instead have the right to withdraw the quantity 14.[84] However, it is noted that Article 14 only applies to 'input errors', that is, errors relating to inputting the wrong data, where an 'automated message system does not provide the person with an opportunity to correct the error', and not other kinds of errors such as a misunderstanding of the terms of the contract.[85]

According to Article 14 of the UN Convention and Article 10 of the EC Directive on Electronic Commerce, before buyers submit the ordering information the website should clearly state that their information is to allow the site owner to decide whether to accept their offer. This allows the site owner to check the product type and cost entered and reject, for example, any offer for a television less than £30 as a minimum price for any television. This application of 'Backstop' logic reduces the cost of mistakes.

In the scenario, if the seller (A) noticed and corrected the price errors before the order was placed, or before the confirmation of acceptance is made, then it would be deemed to be within the above recommendations. But the difference is that contracts made over the world wide web are rarely completed by two humans: a website operates automatically according to a set of instructions, often called a script. It leaves no time for two parties to communicate and negotiate with the conditions, although generally, an acceptance must be communicated to the person making the offer. However,

any person making any offer may waive the general rule and can instead permit acceptance by conduct.[86]

From the author's perspective, a promise to pay over the internet is enough to form the consideration to create a contract. If a clickwrap contract is properly constructed it seems likely that there is consideration to form a binding contract with the viewer. Thus, it makes sense that in the scenario, if the seller (A) delays notification of the price errors, he or she should be responsible for their own negligence, unless they can produce the evidence that the errors occurred due to the computer systems.

4.4.4 Solution II: influence of European Contract Law

According to current legislation there are no clauses concerning the responsibility of mistake, the balance of parties' interest and the reasonable time bar for mistake etc.

How to define 'as soon as possible after having learned of the error' in the UN Convention and EC Directive on Electronic Commerce is the most complicated issue.

In the author's view the appropriate time limit should be defined according to the function of 'withdrawal' of input errors. The fundamental function of 'withdrawal' is to protect the right of the party when the party has unintentionally hit a wrong key or web button and sent a message that he did not intend to send. Provided by appropriate technical means the party should notice the errors **very soon after** inputting the wrong data or clicking the wrong button, a 24 hour time limit seems to be just, depending on the calculation of the starting point of timing. The European Contract Law is consistent with this proposed rule.

The Commission on European Contract Law (also called the Lando-group) presented in 1999 a report called the Principles of European Contract Law (PECL). Many other academic groups have followed up on the Lando-commission and drafted articles related to specific contracts. One of the working groups dealing with specific problems in relation to electronic commerce was established in 2003. The task force's aim is to ascertain that the articles are in harmony with the EC directives related to e-commerce and with other needs that businesses and consumers may have due to the increased use of electronic communication.[87] The report covers six issues. They are, 'input errors', 'cooling off periods', 'unsolicited contracts', 'definitions of sent, received and dispatched', 'definition of writing' and 'definition of signature'.[88] This section will focus on 'input errors' and 'cooling off periods' of the PECL, which complements the EC Directive on Electronic Commerce and the UN Convention on the Use of Electronic Communications in International Contracts.

Article 4:103 of the PECL describes the fundamental mistake as to facts or law, which does not require changing. But changes have been suggested to Article 4:104 as follows:

> Article 4:14 Inaccuracy in Communication
>
> 1 An inaccuracy in the expression or transmission of a statement is to be treated as a mistake of the person which made or sent the statement and Article 4:103 applies.
> 2 Subject to Article 4:103(2), a party concluding a contract at another party's website may avoid the contract for mistake if the other party does not provide effective, accessible and technological means to identify and correct input errors prior to the transmission of a statement.
> 3 The parties cannot derogate from paragraph (2) to the detriment of a consumer.[89]

The above principles express clearly the determination of the errors input which is similar to that in the EC Directive and UN Convention. But neither the EC Directive nor the UN Convention defines the time period of errors input correction. With respect to this point the PECL report further suggests 'cooling off periods (right to withdraw)' in detail.[90] For example, the new suggested Article 2:212(4) expresses clearly that

> the consumer must exercise his right to withdraw from the contract within fourteen days after having concluded the contract, having been informed by the seller or service provider of his right to withdraw and the consequences thereof, and having been supplied with any other data prescribed in any relevant regulation by the European Commission. Whether or not the seller or service provider provided such information, the consumer's right to withdraw expires six months after the date of the conclusion of the contract.[91]

The efforts of the PECL report to unify contracts concluded online are to be welcomed, regardless of whether the PECL electronic contract project can eventually succeed. The two uniform principles of 'input errors' and 'the time period to withdraw' in the report should be highly recommended to electronic commercial transactions at the international legislation level. The current Proposal for a Directive on Consumer Rights, adopted on 28 October 2009 by the European Commission, also introduces identical conditions of 14 days cooling off so that consumers have the right to withdraw the contract, with the web-based withdrawal form, if the contract is concluded online.

Thus, according to the evidence above, in the author's view, a uniform time period of notification of error in electronic communications – in order to retain the right to withdraw input errors – should be within 24 hours in order to promote fairness and certainty in regulating error in electronic communications:

> Option 1: the time period begins when the contract is concluded

and the buyer (including B2B and B2C) is informed of his right to withdraw;

Option 2: the time period begins when an electronic communication becomes capable of being retrieved by the addressee at an electronic address designated by the addressee.

5 Where is the contract made?

With websites and services the concept of establishment, however, is not so straightforward. Popular websites are hosted simultaneously on many so-called duplicating 'mirror services'. They increase resilience, but they may be situated anywhere on the planet. Consequently they may be many thousands of miles from the headquarters of those who control them.[1]

Many electronic contracts are not domestic. One of the great successes of the internet is the creation of a worldwide market place. A trader in Rome can, through a webpage, reach a customer in New York just as easily as one in Sorrento. However, the internet can also create complexity. For example, A's head office is in the UK whilst a team based in China handles technical control of the website and customer support, and credit card processing is conducted in the US. So where is the company established? This cross-border nature of the internet adds a further dimension to electronic contracting, that of international private law, with questions of jurisdiction and choice of law awaiting settlement.[2] That is, the questions will arise as to which law will govern the transaction and which courts will have jurisdiction in the event of a dispute. In the event that a contract is silent on that point, the location where a contract is concluded will be a major factor in determining the choice of law in question.[3]

As internet jurisdiction and choice of law can be very complicated issues, the trader may just want to enter into contracts with certain parties from the local region rather than from any country, avoiding the laws of a particular jurisdiction. In electronic contracting, the place of the contract may be where the offeror is notified of the acceptance of the offer by the offeree, or where the letter of acceptance is posted.

5.1 Place of business

In addressing this issue Article 15 of the Model Law on Electronic Commerce sets out criteria for determining where an electronic message is sent and received. It provides that a message is deemed dispatched at the place where the originator has its place of business, and is deemed received at the place where the addressee has its place of business. In the event that either party has more than one place of business the place of business is the one bearing

the closest relationship to the transaction.[4] If a party does not have a place of business then the party's habitual place of residence is substituted for the place of business.[5]

The UN Convention provides the determination of the location of the parties (Article 6), which is an improvement to the UNCITRAL Model Law on Electronic Commerce. It helps to ascertain jurisdiction, applicable law and enforcement. Its aim is to remove legal obstacles to cross-border electronic commerce. It clearly explicates the definition of 'place of business', 'location of the parties' and 'time and place of dispatch and receipt of electronic communications'. The UN Convention proposes 'place of business' as 'any place maintains a non-transitory establishment to pursue an economic activity other than the temporary provision of goods or services out of a specific location',[6] that is, the place where a party pursues an economic activity through a stable establishment for an indefinite period. Article 6 of the UN Convention regulates the rules of 'location of the parties'. The primary rule is that the parties are taken to be located where they say they are.[7] This is equivalent to 'party autonomy'. In the absence of a party's indicated location the place of business is that which has the closest relationship to the relevant contract.[8] In addition, Article 6(3) provides that 'If a natural person does not have a place of business, reference is to be made to the person's habitual residence'. The UN Convention also clarifies that the location is not merely the place where the equipment and technology are located or a domain name is registered.[9]

In the US the UCITA provides that 'a party is located at its place of business if it has one place of business, at its chief executive office if it has more than one place of business, or at its place of incorporation or primary registration if it does not have a physical place of business. Otherwise, a party is located at its primary residence'.[10]

In China, Article 12 of the Chinese Electronic Signatures Law deals with the main place of business of the sender and the recipient. It states that the place where the data message is sent to or received from shall be deemed to be the main place of business of the sender and the recipient. If there is no main business place the habitual residence of the parties shall be the place of sending or receiving messages.

5.2 Place of performance

Place of performance is another important criterion in determining jurisdiction and applicable law when disputes occur. It can be linked with 'location of the parties', 'place of business' and 'place of dispatch and receipt of electronic communications' under the UN Convention. As discussed earlier, the location of the parties and place of business are regulated by Article 6 of the UN Convention. Article 10(3) of the UN Convention further provides the determination of the place of dispatch and receipt of electronic communications as follows:

> An electronic communication is deemed to be dispatched at the place where the originator has its place of business and is deemed to be received at the place where the addressee has its place of business, as determined in accordance with article 6.

In the old version of the Principles of European Contract Law 1995, Article 2.106 explicitly explains the factors of ascertaining place of performance. It expresses that (1) if the place of performance of a contractual obligation is not fixed by or determinable from the contract it shall be: (a) in the case of an obligation to pay money, the creditor's place of business at the time of the conclusion of the contract; (b) in the case of an obligation other than to pay money, the obligor's place of business at the time of conclusion of the contract. (2) If a party has more than one place of business, the place of business for the purpose of the preceding paragraph is that which has the closest relationship to the contract, having regard to the circumstances known to or contemplated by the parties at the time of conclusion of the contract. (3) If a party does not have a place of business his habitual residence is to be treated as his place of business.

Place of business and habitual residence are the main factors in determining the place of performance in the old PECL. The rules under the Rome I Regulation 2008 are identical to this. For example, Article 4(2) of the Rome I Regulation specifies that 'where the elements of the contract would be covered by more than one of points, the contract shall be governed by the law of the country where the party required to effect the characteristic performance of the contract has his habitual residence'.[11] Compared with the Rome I Regulation, the Brussels I Regulation 2000 provides much more explicit wording in the clarification of place of performance of the obligation that in the case of the sale of goods, the place where the goods were delivered or should have been delivered and in the case of the provision of services where the services were provided or should have been provided.[12] Place of delivery and place of service provided are the performing factors.

Place of performance of an electronic contract is the same as a traditional paper based contract if the performance itself involves physical delivery or presence. The difference lies in the performance that is conducted electronically, i.e. downloading software or an ebook without physical delivery or presence. In this case the time of dispatch and receipt of electronic communications and the determination of the place of computer servers become significant factors to predict and ascertain the actual place of digital performance. Details will be discussed in Part IV.

6 Contemporary issue: electronic battle of forms

Businesses generally wish to contract using their own standard conditions of contract, because they may have drafted their contracts to meet their own product, service, project, technical, commercial and legal requirements.[1] It is called a 'standard contract'. Standard terms are contract terms that one party formulates for use in his contracts generally and provides to other parties for use in their mutual transactions. Typically they are not negotiated but are presented to customers at the conclusion of bargaining over the contract's principal subject matter. Standard terms or general terms are often referred to pejoratively as 'boilerplate'.[2] The boilerplate terms[3] appear on the reverse side of the contract and are usually ignored until a dispute arises. Parties usually reach contracts for international sales of goods utilising standard terms. In standard contracts the party supplying a product or service spells out the terms on which the party does business and which it expects the other party to accept. Sometimes, standard terms designed for use in one country are subject to laws for which they are not designed.[4]

The most crucial issue here is not just the conflict of laws in different countries, but also the determination of whether a contract exists with conflicting terms, whether a particular communication is a rejection of the offer and constitutes a counter-offer, and if the contract was concluded, what the terms of the contract are. This is called a 'battle of forms'. It arises where two companies are in negotiation and as part of their exchanges they each send standard contract forms, but these two sets of forms are incompatible.[5] That is, a battle of forms arises when each party has his own standard terms of trading or business that he wants to prevail over the other party's standard terms.[6]

The 'battle of forms' is one of the most complicated issues in traditional contract law, made even more difficult due to the divergent treatment among jurisdictions. In an English leading battle of form case *Butler Machine Tool Co Ltd v Ex-Cell-O Corpn (England) Ltd*,[7] the sellers offered to sell a machine tool to the buyers, the offer being on the standard terms which 'shall prevail' over any terms and conditions in the buyers' order and which included a price variation clause for increased costs. The buyers' order form contained standard terms materially different from those of the sellers and

stated that the agreed price was fixed. Lord Denning suggested a three-step solution to the battle of forms: first, whether there is an expressed term or implied term from conduct of the last form sent; second, whether the offeree's reply materially affects the contract and he fails to draw the offeror's attention; and third, if there is a concluded contract but the forms vary, the forms can be reconciled so as to give a harmonious result whilst the conflicting terms may have to be scrapped and replaced by a reasonable implication.[8] Lord Denning did not agree to find the existence of the contract first. Instead, he preferred to examine whether there was an agreement on material points, and if there was, determine the agreed and conflicted terms.[9] Professor Forte considered that Lord Denning espoused a more radical approach, because it 'divorces content from formation and does not produce an inevitable finding that the party who fires the last shot must win'.[10]

International legislative instruments have tried to resolve battle of forms in contracts. The Uniform Commercial Code (UCC), the United Nations Convention on Contracts for the International Sale of Goods (CISG), the International Institute for the Unification of Private Law (UNIDROIT), Principles of International Commercial Contracts (PICC), and the Principles of European Contract Law (PECL) have proposed rules of battle of forms that have led to different outcomes.[11] However, the legislations have in common that they follow a 'two-stage' process[12] which first attempts to determine whether there is a contract existing between the parties, and then ascertains it by finding whether the exchanged terms materially differ and what terms prevail.

6.1 International legislation: CISG and PICC

Article 19 of CISG[13] provides that a reply to an offer that contains additions, limitations or other modifications constitutes a counter-offer. The default rule under the CISG is to turn a modified acceptance into a counter-offer that rejects the previous offer. Thus, the original contract does not exist if an acceptance contains additions, limitations or other modifications.

However, the reply purports to be an acceptance, and additional and different terms prevail over the terms of offer if they do not materially differ from those terms of offer. If this reply is the last document to change hands before performance, its terms will bind the parties.[14] Unlike the UCC, §2-207, which will find the existence of a contract as long as the major terms match, the CISG will still allow an offeror to reject an acceptance that contains immaterial variations.[15] However, in contrast with the UCC, §2-207(3), the CISG does not address the question of what happens when conflicting offers and acceptances are exchanged and performance nonetheless begins.[16] The success of the CISG lies in the interpretation of materially altering terms.

6.2 US legislation: UCC

UCC, §2-207[17] states that the contract is concluded even though the acceptance contains additional or different terms. The additional terms of acceptance will become part of the contract, knocking out the terms that materially alter those offered or agreed upon.

The UCC's treatment of battle of forms is far from 'uniform'. While §2-207(1) refers to 'additional or different terms', §2-207(2) only applies to 'additional terms' by providing that 'the additional terms are to be construed as proposals for addition to the contract'.[18] The Cambridge Online Dictionary defines 'different' as 'not the same' while explaining 'additional' as 'extra'.[19] The word 'different' is defined as 'not the same as another or each other' or 'distinct and separate', whilst the Compact Oxford Online English describes 'additional' as 'added, extra, or supplementary'.[20] In the author's opinion, just like 'additional' terms, 'different' terms can alter the original terms materially as well. Under these circumstances the use of the terms 'different' and 'additional' should be treated the same as 'alterations'. However, the concept of 'different' perhaps permits a much broader range of alterations than the definition of 'additional', because whether the offeree or offeror changes some wording of the contract ('different terms') or adds some extra terms and conditions to the contract ('additional terms') it has the same effect on the contract: it makes the contract look different.

§2-207(1) of the UCC is different from the common law, where a 'different' term would create a counter-offer. It mandates that neither 'additional' nor 'different' terms turn an acceptance into a counter-offer; instead, a contract is formed. It is accepted in §2-207(2) that additional terms may become part of the contract except for offer limitations, material alterations or advanced notifications. 'Where documentary exchanges between parties do not disclose a concluded contract', §2-207(3) applies.[21] Under §2-207(3) if the conduct of the buyer and seller is consistent with commercial reality it is sufficient to establish a contract for sale. Terms are those agreed upon by the agreement, whilst the other conflicting terms are left out, and the other provisions of the UCC are supplemented.[22]

6.3 EU legislation: PECL

Differing from the UCC and the CISG, the PICC and PECL separate and treat general conditions conflicts differently from essential terms.[23] Article 2.1.11 and 2.1.22 of the PICC,[24] the same as Articles 2:208 and 2:209 of the PECL,[25] discuss rules separately applying to front-form conflicts (negotiated, essential, or important conditions) and boilerplate conflicts (general conditions).

With regard to conflicting essential terms, both the PICC and PECL are consistent with the CISG in employing that a reply to an offer with additions, limitations or other modifications constitutes a counter-offer, which purports

to be an acceptance if the additional or different terms in reply do not materially alter the offer. The terms of contract are the terms of the offer with the modifications contained in the acceptance. In relation to conflicting general conditions both the PICC and PECL recommend that the contract should be concluded by the agreed standard terms that 'are common in substance'. Thus, the terms of the contract will be formed with the agreed essential terms plus those general terms that 'are common in substance'.[26]

The PICC and PECL attempt to offer both the efficiency and practicality of the CISG in that modified acceptances become counter-offers unless the easily noticed modifications are immaterial, while they apply the 'common in substance' rule to provide a more equitable treatment when differing terms are likely to go unnoticed.[27] The outcomes of conflicting general conditions are the same referring to Article 2.1.22 of the PICC and Article 2:209 of the PECL. The contract is nonetheless formed because both Article 2.1.22 of the PICC and Article 2:209 of the PECL provide that a contract is concluded despite the existence of conflicting general conditions and the general conditions form part of the contract to the extent that they are common in substance.

As analysed above, in summary, the UCC, CISG, PICC and PECL have similarities in that material alteration of an offer is a rejection of an offer and constitutes a counter-offer. However, they are different in relation to whether a valid contract exists despite the existence of conflicting terms and what terms will apply. The CISG, PICC and PECL, compared with the UCC, are more consistent with the ruling of 'different and additional terms'. Another merit of the CISG is that it gives the definition of 'material alterations', which explicitly express the conditions such as the price, payment, quality and quantity of the goods, place and time of delivery, extent of one party's liability to the other or the settlement of disputes. The PICC and PECL are more comprehensive than the UCC and CISG because, as we discussed earlier, they distinguish between essential terms and general conditions.

6.4 Chinese legislation: CLC

The Contract Law of People's Republic of China (CLC) strongly encourages the usage of a standard terms contract. The provisions regulating standard terms are specified in Articles 39 to 41 of the CLC. In accordance with Article 39 parties adopting standard terms in a contract have the duty of fairness, notification and explanation. That is, standard terms shall define the rights and obligations between the parties with fairness. The party who proposes a standard contract shall inform the other party of any exclusion or restriction of liabilities in a reasonable way as well as explain the standard terms upon request by the other party. However, standard terms are not negotiated with the other party when the contract in concluded except for terms depriving the material rights of the other party.[28] Article 41 continues the protection of the parties who are supplied with standard terms, and where

there are two or more kinds of interpretation to the terms, the one that is unfavourable to the party supplying the standard terms shall prevail.

The general issue of battle of forms is governed by the Contract Law of People's Republic of China (hereafter CLC)[29] but without specific provisions directly referring to electronic battle of forms.

The basic article of the battle of forms of CLC is provided by Article 20, which sets four conditions on losing a valid offer. That is, an offer shall lose efficacy if:

1 the notice of rejection reaches the offeror;
2 the offeror revokes the offer in accordance with the law;
3 the offeree fails to dispatch an acceptance before the expiration of the time limit for acceptance;
4 the offeree makes substantial changes to the contents of the offer.

Under the fourth condition in Article 20, 'substantial changes' should be understood as 'material changes'. Article 20 is consistent with Articles 30 and 31, which give more precise details on the validity of substantial changes to offer and acceptance.

With regard to the validity of an offer, Article 30 of the CLC clarifies that the contents of an acceptance shall comply with those of the offer. If the offeree substantially modifies the contents of the offer it shall constitute a new offer. With regard to the validity of an acceptance, Article 31 specifies that if the acceptance does not substantially modify the contents of the offer it shall be effective, and the contents of the contract shall be subject to those of the acceptance, except as rejected promptly by the offeror or indicated in the offer that an acceptance may not modify the offer at all.

The modification relating to the subject matter, quality, quantity, price or remuneration, time or place or method of performance, liabilities for breach of contract and method of dispute resolution shall be regarded as the substantial modification of an offer.[30] This is compatible with the UCC, CISG, PICC and PECL – that material alteration of an offer is a rejection of an offer and constitutes a counter-offer.

6.5 How is 'battle of forms' resolved in electronic contracts?

However, the battle of forms will be even more complicated in electronic contracts because of the features of instantaneous electronic communications. In electronic contracts battle of forms will be related to the issues of dispatch and receipt of an electronic communication,[31] validity of offer and acceptance, availability of contract terms,[32] and errors in electronic communications.[33]

When a buyer submits an order on the seller's website, the seller is able to present its standard terms and conditions to the buyer. Then there are three possibilities: firstly, the buyer can simply accept the standard form, so the contract is concluded with the standard terms of the seller. Secondly, the

buyer can reply to the seller with a notice of another set of standard terms that are posted at a designated URL (Uniform Resource Locator). For example, the buyer might reply to the seller asserting that 'assent is withheld unless the seller assents to the terms and conditions located at http://www.company.com/terms&conditions.html'.[34] Thirdly, the buyer may have no immediate indication of a failed attempt to communicate, and the seller may well only receive a message saying that the email has not been delivered at some time later.[35]

Under the first possibility it is equivalent to a clickwrap agreement presenting standard terms. However, the second possibility is the battle of the URLs in the contract. If an acceptance is followed by a separate email or telephone call, the separate email or telephone call should become part of the contract,[36] if it does not materially alter the original contract. If an agreement is only partially integrated, extrinsic evidence of consistent additional terms is admissible.[37]

According to the previous analysis of rules of battle of forms and the above discussion of specific electronic battle of forms, in the author's view, in electronic contracting, the combination of the ruling of the CISG, PICC and PECL will be practical and appropriate. This means that an electronic acceptance that contains additions, limitations or other modifications is a rejection of the offer and constitutes a counter-offer. However, if the additional or different terms in the general conditions of the acceptance do not materially alter the offer they form part of the contract to the extent that they are common in substance, or otherwise as the parties agree.

Summary

In summary, because of the unique features of the internet, existing regulatory schemes designed to regulate traditional technologies and transactions may not be accurate and sufficiently applicable to electronic contracting. Thus, the solution would be to either apply existing laws and interpret them in a way that reflects the complexities of online contracting or, where appropriate, adopt new regulations or directives to address the development of technology and newly raised disputes. It is worth noting Professor Ramberg's argument that EC Directives are not efficient and it is difficult to reach consensus and harmonisation of laws because they are not based on a voluntary basis in their implementation, and the tradition of not stipulating the sanctions and effects causes the directives to become implemented differently in the different Member States.[38] In the author's opinion, new model laws and conventions governing issues of electronic commercial transactions are necessary because they set simple, basic and core principles at the international level, which is, in return, essential to provide a uniform legal infrastructure for global electronic commercial transactions.

The EC Directive on Electronic Commerce (E-Commerce Directive), the US Uniform Electronic Transaction Act (UETA) and the China Electronic

Signatures Law have provided a legal infrastructure to national or regional electronic commerce markets. At the international level, the UNCITRAL Model Law on Electronic Commerce and the UN Convention on the Use of Electronic Communications in International Contracts (the UN Convention) have made great efforts to modernise and harmonise international electronic commerce laws. They have in common that they employ the principle of functional equivalency for a record or signature in an electronic form. Different from the others, the EC Directive on Electronic Commerce particularly requires that 'the service provider has to acknowledge the receipt of the recipient's order without undue delay and by electronic means'.[39] Professor Ramberg argued that there was no need to have a legal requirement of confirmation under the EC Directive on Electronic Commerce because there is no general rule that a contract be confirmed, and when the contract is already at hand the confirmation has no legal effect at all.[40] In the author's view the ruling of confirmation of the receipt of the recipient's order is necessary, because it will certainly boost the confidence of electronic commercial transactions and give parties the certainty that their corresponding electronic messages have been successfully delivered. However, acknowledgement of receipt is not equivalent to an acceptance, although it might perform the function of acceptance in clickwrap agreements.

The UN Convention complements the UNICTRAL Model laws on electronic commerce and electronic signatures. It enhances legal certainty and commercial predictability of electronic contracting by determining electronic authentication methods, place of business, location of parties, time and place of dispatch and receipt of electronic communications, (automated transactions).[41] The UN Convention uniforms the determination of the location of the parties and time and place of dispatch and receipt of electronic communications where there are various versions of wording in the EC Directive on Electronic Commerce, the UNCITRAL model laws and the UETA.

The UN Convention is a great success in the above aspects. However, the remaining key criticisms of the UN Convention are fivefold. Firstly, there is a need to define 'electronic contracting'. When giving the definition, three concepts should be combined: electronic communications; automated transactions; and data messages.

Secondly, it is necessary to determine when the offer and acceptance take effect. From a legal point of view there is no need to distinguish non-instantaneous contracting, such as emailing, from instantaneous contracting, such as clickwrap agreements, because although it is non-instantaneous contracting by email it is still much quicker than normal postal services. In addition, using different email servers and different internet services can result in different speeds of sending and receiving messages – some emails might be like instantaneous messages so it would be more difficult to reach consensus and efficient harmonisation of the rule to different standard users and make it fair. Therefore, the 'acceptance' or 'receipt' rule would be a more sensible application to electronic contracting.

Thirdly, the UN Convention lacks provisions regulating individual communications of e-contracts, which become a noteworthy issue in electronic transactions. With the improvement of IT industry and e-commerce service online companies can offer customers many more choices when they order products or services online, by pressing different functional buttons and inputting different variations. By suggesting the doctrine of individual communications in concluding an e-contract, the UN Convention should employ 'party content before concluding an e-contract' as a condition. It means that it should be compulsory for parties to be aware of communications and for the servers to provide functions for parties to express their contents.

Fourthly, the technology neutral approach and the time measure of notification of error in electronic communications should be employed in 'errors in electronic communication', because new techniques of amending input errors or wrong messages have been developed dramatically, such as the 'recall or replace a message you've already sent' function in Microsoft Exchange Server, which may conflict with the existing rule of 'duty of notification as soon as possible' under the UN Convention.

Lastly, the UN Convention is silent on battle of forms in electronic commercial transactions, which, in the author's view, should be included since it will occur more often when more and more large or medium-size firms get involved in e-trading. According to the discussion earlier the traditional rules contained in the UCC, CISG, PICC, PECL and CLC should be combined to apply to online battle of forms; that is, electronic acceptance – which contains additions, limitations or other modifications – is a rejection of the offer and constitutes a counter-offer. However, if the additional or different terms in the general conditions of the acceptance do not materially alter the offer, they form part of the contract to the extent that they are common in substance, or otherwise the parties agree.

Overall, nations have made efforts to expedite the development of electronic commerce but different approaches or methodologies have been adopted. It is notable that the US is attempting to drive the international marketplace into the internet age, while the EU approach appears to be more focused on growing the internal marketplace. China, as the second largest internet users' country, has been learning from the Western legislative experience and establishing new laws to adapt to the online market, although there are still additional areas to cover, especially issues regarding electronic cross-border jurisdiction. However, China, along with the rest of the international community, is searching for a harmonious global solution. Nevertheless, regulation, model law or convention should be minimal, clear and simple, and predictable and consistent.[42] But it is necessary to bear in mind that the process of modernisation and harmonisation of the performance of e-contracts and choice of laws through an international instrument is lengthy and arduous and involves the infusion of a prodigious amount of expertise, time and money.

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

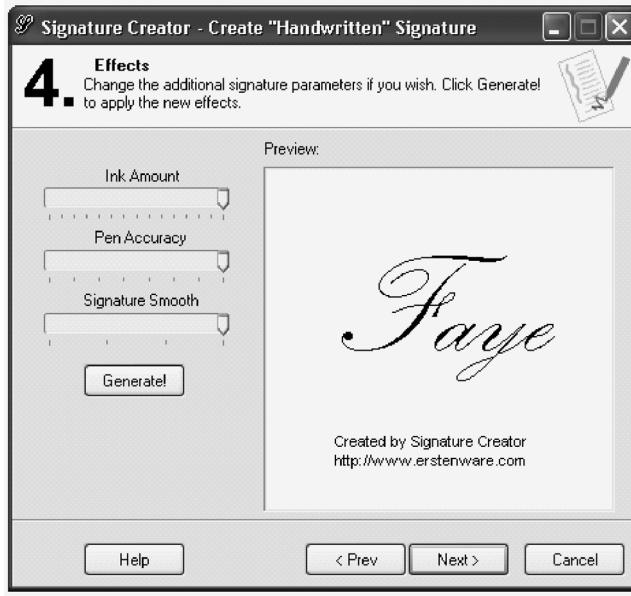

Figure 7.1 Signature Creator 1.12 description.[23]

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.

Part IV

Dispute resolutions

10 Resolving electronic commercial disputes

Businesses, through the use of the internet, can enter into electronic sales contracts with other businesses located in different countries or sell data to a third country easily and quickly. The potential for disputes in the validity of cross-border electronic contracts and the protection of transborder data privacy, is, obviously, much greater than in a paper-based environment where a high degree of commercial contracts are domestic in nature. The determination of internet jurisdiction and applicable law could be much more complicated and uncertain because online contracting is often executed in several places and it is difficult to ascertain the principal place.

At the international level there are no specific rules in the model laws and conventions dealing with internet jurisdiction and choice of law. The UNCITRAL Model Law on Electronic Commerce and the UN Convention on the Use of Electronic Communications in International Contracts do not contain any jurisdiction or choice of law provisions, but provide the measures of the time and place of dispatch and receipt of data messages or electronic communication[1] and the location of the parties.[2] For example, the connecting factors on parties' business location such as 'the place of business', 'the closest relationship to the relevant contract, the underlying transaction or the principal place of business', or 'habitual residence', may be used to determine internet jurisdiction and choice of law.

The EU, as stated in Recital 23 and Article 1(4) of the EC Directive on Electronic Commerce, does not establish any additional rules on private international law with regard to jurisdiction and choice of law.[3] There is also no particularised internet jurisdiction and choice of law legislation in China and the US.

10.1 Internet jurisdiction[4]

Jurisdiction is one of the main subject matters within the region of private international law (also called 'conflict of laws'). Conflict of jurisdiction means several courts may have rights to hear a particular case. When conflict occurs there is a need to ascertain which court is fully entitled to exercise the jurisdiction.

Internet jurisdiction added a new dimension to courts exercising jurisdiction in the late 1990s when disputes, such as electronic commercial transactions or other internet-related subject infringement, happened. Whether the traditional rules of jurisdiction can still be sufficient to determine internet jurisdiction has been questioned and debated.

10.1.1 EU rules applied in cyber jurisdiction

In the EU the Brussels I Regulation (EC No 44/2001),[5] the replacement of the 1968 Brussels Convention, is deemed to be:

> a highly successful instrument, which has facilitated cross-border litigation through an efficient system of judicial co-operation based on comprehensive jurisdiction rules, coordination of parallel proceedings, and circulation of judgments. The system of judicial co-operation laid down in the Regulation has successfully adapted to the changing institutional environment (from intergovernmental co-operation to an instrument of European integration) and to new challenges of modern commercial life.[6]

The above statement is concluded by the Commission's Report on the Review of the Brussels I Regulation on 21 April 2009. There is no doubt that the Brussels I Regulation plays a very significant role in harmonising judicial co-operation between Member States and its achievement in facilitating cross-border litigation cannot be undermined. However, it is probably arguable that whether the Brussels I Regulation has successfully adapted to new challenges of modern commercial life, in particular, new judicial issues on internet-related cases, Article 23(2) of the Brussels I Regulation is the only rule that explicitly acknowledges agreements by electronic means.

The Green Paper, issued on 21 April 2009, accompanies the Commission's Report to launch a broad consultation with eight questions on the review of the Brussels I Regulation:[7]

Question 1: the abolition of intermediate measures to recognise and enforce foreign judgments (*exequatur*);
Question 2: the operation of the Regulation in the international legal order;
Question 3: choice of court agreements;
Question 4: industrial property;
Question 5: *lis pendens*[8] and related actions;
Question 6: provisional measures;
Question 7: the interface between the Regulation and arbitration; and
Question 8: other issues.

The main function of these questions is to collect opinions on how to remove

obstacles to a free circulation of judgments, enhance certainty of cross-border jurisdiction relating to one of the parties domiciled in a third country rather than Member States, and avoid parallel proceedings in different Member States. Questions 2, 3 and 5 are connected and interacted, especially Questions 2 and 3 with regard to international jurisdiction issues. Although the concerns raised in the Review of the Brussels I Regulation do not directly point to the question of determination of internet jurisdiction, internet jurisdiction is a cross-border issue and, as such, ensuring the smooth operation in the international legal order will reflect on facilitating internet jurisdiction.

Choice of court clause or agreement

A well-drafted contract will usually insert a choice of jurisdiction or court clause. This is often referred to as an 'exclusive' clause, providing that all disputes between the parties arising out of the contract must be referred to a named court or the courts of a named country.[9] On 1 April 2009 the European Council signed on behalf of the European Community the Hague Convention on Choice of Court Agreements[10] concluded on 20 June 2005 (hereafter the Choice of Court Convention).[11] The Choice of Court Convention shall 'apply in international cases to exclusive choice of court agreements concluded in civil or commercial matters'.[12] So when the EU accedes to the Choice of Court Convention the European Commission shall declare clearly the meaning of 'international cases' and that a choice of court agreement can only be governed by the Choice of Court Convention if one of the parties is not domiciled in an EU Member State. Otherwise, it may conflict with Article 23 of the Brussels I Regulation as Article 23(1) applies when at least the parties, one or more of whom is domiciled in a Member State, have agreed that the courts of a Member State are to have jurisdiction over disputes arising in connection with a particular legal relationship.

In other words, Article 23 of the Brussels I Regulation authorises parties, one or more of whom are within Member States, to enter into an agreement designating the court or courts to determine such disputes. The chosen courts can be general courts or specific courts of a country. For example, Company A (in Italy) and Company B (in Germany) have agreed a jurisdiction clause 'disputes must be referred to the courts of Germany' in their electronic contracts of sale. Under these circumstances German courts are designated to have jurisdiction over A and B's disputes. However, if later on, A and B made another distribution contract without a jurisdiction clause (the sales contracts and the distribution agreement are different legal relationships), then the original jurisdiction clause in the sale contract does not confer jurisdiction with regard to a dispute arising under the distribution contract.[13] If the jurisdiction clause includes a choice of a particular court, Article 23 is to confer jurisdiction on that court, but not on other courts in the same country. However, A and B can also choose the other courts, for instance the French

court, instead of the Italian or German courts, to hear the case, because Article 23 does not 'require any objective connection between the parties or the subject matter of the dispute and the territory of the court chosen'.[14] Moreover, A and B can also conclude a further exclusive jurisdiction agreement varying the earlier agreement, because Article 23 is based on the principle of party autonomy and it does not prevent parties from changing their decisions.[15]

However, Article 23(3) includes an exemption to parties, none of whom is domiciled in a Member State. In this situation the chosen courts have discretion to determine the existence and exercise of their jurisdiction in accordance with their own law.[16] The courts of the other members shall have no jurisdiction over the disputes unless the chosen court or courts have declined jurisdiction.

As recognised by Article 23(2) of the Brussels I Regulation, 'any communication by electronic means which provides a durable record of the agreement shall be equivalent to writing'.[17] In the author's view this clause implies that a contract stored in a computer as a secured word document (i.e. a read-only document or document with entry password), or concluded by email and a clickwrap agreement falls within the scope of Article 23(2) of the Brussels I Regulation. In the e-contracting cases, to insert a choice of jurisdiction clause in the standard terms and conditions on the website can avoid further ambiguity about which court has jurisdiction when disputes arise. For example, the website owner can incorporate a choice of jurisdiction clause into an interactive clickwrap agreement that the buyer needs to click the 'I agree' button to assent to.[18]

Just like ordinary contracts, courts will determine jurisdiction of an online contract according to three main types of jurisdiction rules in the Brussels I Regulation: general jurisdiction, special jurisdiction and exclusive jurisdiction.

General jurisdiction

The general jurisdiction rule under the Brussels I Regulation is that defendants who are domiciled in one of the contracting states shall be sued at the place of their domicile.[19] Under Article 2 of the Brussels I Regulation, persons domiciled in a Member State shall, whatever their nationality, be sued in the courts of that state. Furthermore, domicile rules within the Brussels I Regulation govern the domicile of individuals[20] and domicile of corporations.[21] With contracts made over the internet it is difficult to determine where the party is domiciled, even though the plaintiff can identify the party and locate the transaction.[22] Article 59(1) of the Brussels I Regulation provides that, as regards natural persons, in order to determine whether a party is domiciled in a particular Member State, the court shall apply the law of that state. Article 60(1) lays down that for the purposes of the Brussels I Regulation a company or other legal person or association of natural or

legal person is domiciled at the place where it has (1) its statutory seat or (2) its central administration or (3) its principal place of business.

On the internet, since the decision of the e-transaction might be made following discussion via video conferencing between senior officers who reside in different states, it has become more difficult to ascertain the location of the central administration.[23] According to the UN Convention on the Use of Electronic Communications in International Contracts (the UN Convention), 'the location of the parties'[24] is defined as 'a party's place of business'.[25] If a natural person does not have a place of business, the person's habitual residence should be deemed as a factor to determine jurisdiction.[26] The UNCITRAL Model Law on Electronic Commerce is the same as the UN Convention, providing that 'if the originator or the addressee does not have a place of business, reference is to be made to its habitual residence'.[27] In the author's view, the person's habitual residence on the internet occasion should be treated the same as the traditional offline rule that general jurisdiction should be connected to the habitual residence of the defendant but not the claimant.

Furthermore, according to the UN Convention, if a party does not indicate his place of business and has more than one place of business, then the place of business is that which has the closest relationship to the relevant contract.[28] The closest connecting factors are those that occur before or at the conclusion of the contract.[29] In the author's opinion, these factors are no different from the offline world, which would also relate to statutory seat, central administration or principal place of business. As a person or legal person doing electronic commerce, his/her statutory seat, central administration or principal place of business can be checked by the claimant, and the result can be found according to some connecting factors such as the registration of the defendant's business, licences, electronic payments and places of delivery of goods or services. This would lead to the following issue: special jurisdiction.

Special jurisdiction

Article 5 of the Brussels I Regulation derogates from the general principle contained in Article 2, which gives the claimant the opportunity to proceed against the defendant in a Member State in which the defendant is not domiciled. Under this provision it contains seven matters, one of which, Article 5(1), deals with matters relating to a contract. This general rule does not apply to insurance, consumer and employment contracts.[30]

How to ascertain 'the place of performance of the obligation in question'[31] is the focal point of how to determine jurisdiction. The place of performance, according to Article 5(1)(b), is the place of delivery of goods (or where it should have been delivered), or the place where the services were provided or should have been provided. Since the place of delivery is a close linking factor to determine special jurisdiction, an electronic contract is no different

from a paper-based contract when the contract itself involves physical delivery of goods. The difficulty in applying Article 5(1) lies in the interpretation of whether multiple places of delivery are within the scope of Article 5(1).

Unfortunately what Article 5(1)(b) does not expressly address is that posed by the situation where, as regards a contract for the sale of goods, there is more than one place of delivery or, in relation to a contract of services, there is more than one place of performance. Problems with regard to multiple places of delivery of goods or provision of services,[32] can be divided into two categories: one is, different obligations have different places of delivery, and the other is that the relevant obligation has several places of delivery.

At the first category, there are two possibilities: first, disputes concern more than one obligation. Article 5(1) allocates jurisdiction to the courts for each place of performance with regard to the dispute arising out of the obligation, which should have been performed at that place.[33] Second, cases involve two obligations with one principal obligation. The courts for the place of performance of the principal obligation have jurisdiction over the whole claim.[34]

At the second category, there are also two possibilities: first, as noted by the most recent case *Color Drack GmbH v Lexx International Vertriebs GmbH*,[35] there is a query about 'whether the first indent of Article 5(1)(b) of the Brussels I Regulation applied in the case of a contract for the sale of goods involving several places of delivery within a single Member State',[36] and if so, 'whether the plaintiff could sue in the court for the place of delivery of its choice'[37] among all places of deliveries. The Court ruled that the applicability of the first indent of Article 5(1)(b), where there are several places of delivery within a single Member State, complies with the regulation's objective of predictability, and proximity underlying the rules of special jurisdiction in matters relating to a contract.[38] Because the defendant should expect, when a dispute arises, that he may be sued in a court of a Member State other than the one where he is domiciled. Although the defendant might not know exactly which court the plaintiff may sue him in, he would certainly know that any court which the plaintiff might choose, would be situated in a Member State of performance of the obligation. As to the question of whether the plaintiff can sue in a court of its own choice under Article 5(1)(b), the Court ruled that for the purposes of application of the provision, the place of delivery must have the closest linking factor between the contract and the court, and 'in such a case, the point of closest linking factor will, as a general rule, be at the place of the principal delivery, which must be determined on the basis of economic criteria'.[39] If all places of delivery are 'without distinction', and 'have the same degree of closeness to the facts in the dispute',[40] the plaintiff could sue in the court for the place of delivery of its choice.

This first query leads to the second consideration: if the places of delivery were in different Member States, will Article 5(1)(b) still apply? Where the

relevant obligation has been, or is to be, performed in a number of places in different Member States, following the Advocate General's opinion, Article 5(1)(b) does not apply to this situation as the objective of foreseeability of the Brussels I Regulation could not be achieved;[41] that is, if a single place of performance for the obligation in question could not be identified for the purpose of this provision,[42] then the claimant should turn to Article 2 of the Brussels I Regulation, according to which the court with jurisdiction is that of the domicile of the defendant.

In B2B electronic contracting disputes can Article 5(1) still apply? If so, how can Article 5(1) be employed to resolve internet jurisdiction disputes? To answer these questions it will first be necessary to determine whether an electronic contract is for the sale of goods, or the provision of services. Next, a distinction will be made between physical goods and digitised goods, physical services and digitised services, and physical performance and digitised performance. This will make it possible to determine the differences and similarities concerning the place of performance between online and offline contracting.

Firstly, is there a contract for the sale of goods, the provision of services or neither? Generally, goods can be ordinary goods with physical delivery and digital goods with performance over the internet, such as digital books, online journals and software programs. With regard to software programs, there is academic authority in favour of the proposition that software transferred online constitutes 'goods' for the purposes of the United Nations Convention on Contracts for the International Sale of Goods (CISG).[43] However, carriage of goods by sea, the provision of financial services, providing internet access to recipients or designing a website for a company should all be categorised as services. In addition, programming software that meets the buyer's specific needs should be regarded as providing services. Sometimes, in a complex software development project, a piece of software program can be broken down into self-contained sections so that when there is payment by instalments on completion of milestones, payment will be due from the buyer on completion of each milestone within the framework of a software development contract.[44]

Secondly, how should digitised goods be distinguished from other products? Digitised products are intangible. Intangible property is, by its nature, not physically located in a particular state.

However, the fact that a party has downloaded digitised products onto his computer, so that they are located on his hard drive, does not mean that the relevant *situs* is the place where the computer is presently located. Rather, we must consider the more complex question of where digitised products were located at the time of the purported dealing with them.[45]

Thirdly, what can be the place of performance of the obligation in question in cyberspace? As discussed before, the place of delivery between businesses is usually included in the contract of sale.[46] However, it becomes complicated when parties do not indicate the place of delivery in their contract, because it

might involve multiple places of delivery and services might also be provided by the seller's agencies. Furthermore, it would be even more complex when the transaction involves the delivery of digitised goods, as there are a number of places where electronic transactions are processed, for example, place of dispatch and receipt, the place where the seller has a specified personal connecting factor and the place where the recipient (i.e. the buyer) has a specified personal connection.

According to Article 5(1)(b) of the Brussels I Regulation, the place of performance should be deemed to be the place of delivery. Since it is very difficult to ascertain the place of performance with digitised goods involving online delivery, in the author's opinion both the sender's and recipient's place of business could be considered connecting factors depending on the characteristics of commercial transactions. In other words, in B2B and B2C electronic commercial transactions the closest connecting factors might be treated differently. However, the recipient's place of business as a connecting factor seems to be compatible with the US jurisdiction tests as discussed below.

10.1.2 US jurisdiction tests

Due to the fact that US companies are at the forefront of internet technology, litigation regarding e-commerce in the US is more advanced than anywhere else in the world. On 19 January 2009, the US, like the EU, signed the Hague Convention of Choice of Court Agreements.[47] If both the US and EU accede to the Hague Convention it will facilitate the harmonisation of judicial agreements and procedures between the two states.

Similar to the EU Brussels regime (general and special jurisdiction), there are two types of jurisdiction in the US: general and specific. General jurisdiction is jurisdiction over the defendant for any cause of action, whether or not related to the defendant's contacts with the forum state; whereas specific jurisdiction exists when the underlying claims arise out of, or are directly related to, a defendant's contacts with the forum state.[48]

The above notion comes from the famous case *International Shoe Co v Washington*,[49] which indicated that the minimum contacts test has both a general and a specific component.[50] What is meant by 'minimum contacts'? It is a requirement that must be satisfied before a defendant can be sued in a particular state. In order for the suit to go forward in the chosen state, the defendant must have some connections with that state. For example, advertising or having business offices within a state may provide minimum contacts between a company and the state.

General jurisdiction

Under the most commonly employed minimum contacts test, general jurisdiction is usually premised on 'continuous and systematic' contacts

between the defendant and the forum so as to make the defendant amenable to jurisdiction without regard to the character of the dispute between the parties.[51] It is clear that if the contacts that are unrelated to the dispute ('unrelated contacts') meet the threshold of being 'continuous and systematic', the defendant is amenable to general jurisdiction based upon its contacts with the state.

The most difficult issue in relation to general jurisdiction is the amount of unrelated contacts needed to subject a defendant to *in personam* jurisdiction.[52] That is, the defendant has some continuing physical presence in the forum, usually in the form of offices. There is a question whether 'mere' residence, as opposed to domicile or nationality, can be a sufficient connection for the exercise of general jurisdiction over an individual defendant.[53] The Second Restatement states that a defendant's residence is sufficient for the exercise of general jurisdiction 'unless the individual's relationship to the state is so attenuated as to make the exercise of such jurisdiction unreasonable'.[54] Thus, general jurisdiction results from a party's continuous, systematic and ongoing ties to a certain forum.[55]

Specific jurisdiction

However, specific jurisdiction turns upon the character of the dispute ('related contacts'). That is, if the contact is related to the cause of action, such related-contact jurisdiction is specific jurisdiction, because (unlike general jurisdiction) it is dependent upon the character of the dispute.[56] Specific jurisdiction is often used when a party's contacts do not fulfil the general jurisdiction criteria, and permits the court to assert jurisdiction over parties to a dispute arising from the parties' contacts with the state involved.[57] Due to the requirement that the contacts are 'related' to the dispute, those contacts may well suffice for jurisdiction in the lawsuit at hand, but may not in another lawsuit relating to the defendant's activities in another state.[58] Thus, determining whether specific jurisdiction exists in a particular case depends upon two separate considerations – the first is whether the contacts are 'related' to the dispute. The second, assuming that the contacts are so related, is whether the contacts are 'constitutionally sufficient'.[59]

For the last few years, US courts, both state and federal, have been wrestling with the problematic issue of personal jurisdiction in the context of internet-related activities. In deciding these cases US courts have been reluctant to view the mere general availability of a website as a 'minimum contact' sufficient to establish specific personal jurisdiction over a non-resident defendant, at least in the absence of other contacts with the forum state.[60] Whether a defendant can be subject to specific jurisdiction in contact cases depends on the entire course of dealing, including 'prior negotiation and contemplated future consequences' establishing that 'the defendant purposefully established minimum contacts with the forum'.[61]

In practice, when trying to determine whether it has personal jurisdiction

over a non-resident defendant, the US court will use a two-step test. First, the court will examine the state's long-arm statute in order to determine whether there is a statutory basis for allowing that plaintiff to sue the defendant in that forum. In the second step, the court looks for some acts or activities by which the defendant has purposefully availed himself or herself of the privilege of conducting business in that state to such an extent that the defendant should reasonably anticipate being sued there.[62] The second step plays a large role in the jurisdiction calculus, that is, 'purposefully' and 'reasonableness'.

In addition, specific jurisdiction can also be examined by two factors: exercise of jurisdiction is consistent with these requirements of 'minimum contacts' and 'fair play and substantial justice'. These can firstly be determined by where the non-resident defendant has purposefully directed his activities or carried out some transaction with the forum or a resident thereof, or performed some act by which he purposefully availed himself of the privileges of conducting activities in the forum, thereby invoking the benefits and protections of its laws; secondly, the claim arises out of or relates to the defendant's forum-related activities; and thirdly, the exercise of jurisdiction is reasonable.[63]

In the *Zippo* case, the Western Pennsylvania District Court expanded on the International Shoe 'minimum contact test' by stating that personal jurisdiction for e-commerce companies should be dealt with on a 'sliding scale'.[64] That is, the 'minimum contacts' test sets forth the due process requirements that a defendant, not present in the forum, must meet in order to be subjected to personal jurisdiction: 'he must have certain minimum contacts with it such that the maintenance of the suit does not offend "traditional notions of fair play and substantial justice" '.[65] *Zippo Mfg Co v Zippo Dot Com Inc*[66] is emerging as the seminal case on whether an internet website provides the minimum contacts necessary to establish jurisdiction. *Zippo* introduced a sliding scale to analyse the contacts of potential defendants created by internet websites. In determining the constitutionality of exercising jurisdiction the *Zippo* court focused on the 'nature and quality of commercial activity that an entity conducts over the Internet'.[67]

The sliding scale approach can be divided into three categories – first: active websites. The defendant enters into contracts with residents of a foreign jurisdiction that involve the repeated transmission of computer files over the internet;[68] these are grounds for the exercise of personal jurisdiction. Second: passive websites. Passive websites merely provide information to a person visiting the site. They may be accessed by internet browsers, but do not allow interaction between the host of the website and a visitor to the site. Passive websites do not conduct business, offer goods for sale, or enable a person visiting the website to order merchandise, services, or files. The defendant has simply posted information on a passive internet website which is accessible to users in foreign jurisdictions. This is not a ground for the exercise of personal jurisdiction. Third: interactive websites. Interactive websites make up the middle of the sliding scale where a user can exchange

information with the host computers. In this middle scale, jurisdiction should be determined by the 'level of interactivity and commercial nature of the exchange of information that occurs on their web site'.[69] Factors such as online contracting (found on most e-commerce sites) can show a high level of interaction leading to the exercise of jurisdiction. This is the crucial point of the sliding scale analysis. If the activities occurring on a defendant's website lean more towards the passive side of the scale, personal jurisdiction will not be applied. If, however, the activity slides toward the active side of the scale, personal jurisdiction will likely be upheld.[70]

As discussed above, the most developed doctrine of US jurisdiction is the *Zippo* sliding scale which encourages inquiry into the level of interactivity of a website. However, in order to avoid it falling into the middle of the scale one would have expected the court to provide a rough definition of 'interactivity', but it did not.[71] Moreover the *Zippo* test, with its emphasis on the level of interactivity inherent to a website, has become less relevant given that almost all commercial sites are now 'at least highly interactive, if not integral to the marketing of the website owners'.[72]

US courts, in accordance with jurisdictional developments abroad, have further developed an alternative approach to determining jurisdiction in e-commerce: an 'effects' test, based on the Supreme Court's decision in *Calder v Jones*.[73] It permits states to exercise jurisdiction when the defendants intentionally harm forum residents. In applying this 'effects' test to internet cases, US courts focus on the actual effects the website has in the forum state rather than trying to examine the characteristics of the website or web presence to determine the level of contact the site has with the forum state.[74] However, an 'effect' test will more easily apply to injuries in tort to individuals where injury is localised or intent can be inferred, but not when e-commerce cases involve corporations.[75] Because determining where a larger, multi-forum corporation is 'harmed' is a difficult prospect[76] the court noted that the 'effects' test does not 'apply with the same force' to a corporation as it does to an individual because a corporation 'does not suffer harm in a particular geographic location in the same sense that an individual does'.[77]

Questioning the utility of the *Zippo* and 'effects' tests, some US courts have focused on whether there was 'something more' needed for the exercise of jurisdiction. Courts further introduced the 'targeting test'.[78] The requirement of the 'targeting test' is satisfied 'when the defendant is alleged to have engaged in wrongful conduct targeted at a plaintiff whom the defendant knows to be a resident of the forum state'.[79] It has been argued that the targeting-based test is a better approach for the courts to employ than the sliding scale test in *Zippo* when determining jurisdiction in cases involving internet-based contacts. The targeting test, unlike the other one, places greater emphasis on identifying the intentions of the parties and the steps taken to either enter or avoid a particular jurisdiction.[80] Further, the advocates of the targeting test view it as a better and fairer approach for determining whether the defendant reasonably anticipated being hauled into

a foreign court to answer for his activities in the foreign forum state.[81] This determination is central to the due process analysis articulated by the US Supreme Court in *World-Wide Volkswagen*: '[T]he defendant's conduct and connection with the forum State are such that he should reasonably anticipate being hauled into court there'. The Due Process Clause, by ensuring the 'orderly administration of the laws', gives a degree of predictability to the legal system that allows potential defendants to structure their primary conduct with some minimum assurance as to where that conduct will and will not render them liable to suit.[82]

So how can we ascertain the 'targeting' approach in electronic contracts?

Firstly, it is based on the intention of the defendant: the defendant must 'direct' electronic activity into the forum state. Unlike the *Zippo* approach 'a targeting analysis seeks to identify the intentions of the parties and to assess the steps taken to either enter or avoid a particular jurisdiction'.[83] It requires that a defendant specifically aims its online activities at a forum to come under the jurisdiction of that state.[84] This will give courts a solid conceptual basis: a 'deliberate or intended action' from which to tackle sophisticated cases and produce consistent results.[85] Secondly, the defendant must intend to engage in business or other interactions ('something more') in the forum state. Thirdly, the defendant must engage in an activity that created under the forum state's law a potential cause of action with regard to a person in the forum state.

Although the targeting approach provides consistency and legal certainty it does not totally preclude the 'American propensity toward individualized justice'.[86] Overall, among the three measuring mechanisms discussed above, the 'targeting' approach gives more legal certainty over determining internet jurisdiction.[87]

10.1.3 Chinese legislation on internet jurisdiction

There is no particularised internet jurisdiction legislation promulgated in China. The general international or national rules covering issues of jurisdiction are currently being used. Jurisdiction agreements concluded through electronic means should be regarded as equivalent to those in writing, on the basis of the Chinese Contract Law and the Chinese Electronic Signature Law. Chapter II of the Civil Procedure Law of the People's Republic of China[88] deals with the issues of jurisdiction to adjudicate and also covers international arbitration and judicial assistance (e.g. enforcement of foreign courts' judgments or the awards of a certain arbitration tribunal).

The Civil Procedure Law, unlike relevant laws in the EU and US, does not address the jurisdiction provision by focusing on general and special principles. Overall, it governs jurisdiction of contracts by providing that 'a lawsuit initiated for a contract dispute shall be under the jurisdiction of the people's court in the place where the defendant has his domicile or where the contract is performed'.[89] Currently, there are three core interpretations of

the Civil Procedure Law issued by the Supreme Court to help implement jurisdiction issues. They are: the 1992 Opinions of the Supreme Court on the Implementation of the Civil Procedure Law; the 1998 Regulations of the Supreme Court Regarding Some Questions on the Enforcement of Judgments; and the 2002 Regulations of the Supreme Court Regarding Some Questions on International Jurisdiction in Civil and Commercial Matters.

The Chinese Civil Procedure Law, just like the EU and US, employs 'party autonomy'. Article 25 of the Civil Procedure Law regulates choice of court issues and is in favour of 'party autonomy'. It states that:

> the parties to a contract may choose through agreement stipulated in the written contract the people's court in the place where the defendant has his domicile, where the contract is performed, where the contract is signed, where the plaintiff has his domicile or where the object of the action is located to have jurisdiction over the case, provided that the provisions of this Law regarding jurisdiction by level and exclusive jurisdiction shall not be violated.[90]

Article 243 deals with lawsuits brought against a defendant who is not domiciled in the People's Republic of China concerning a contractual dispute or other disputes over property rights and interests. The defendant shall be sued in the courts where the contract is signed or performed, where the object of the action is located, where the defendant's distrainable property is located, where the infringing act takes place, or where the representative agency, branch or business agent is located.

Moreover, Article 244 of the Civil Procedure Law specifically applies to international cases, requiring that parties should choose the court which has substantial connection with the disputes.[91] Article 246 of the Civil Procedure Law provides that 'Lawsuits initiated for disputes arising from the performance of contracts for Chinese-foreign equity joint ventures, or Chinese-foreign contractual joint ventures, or Chinese-foreign cooperative exploration and development of the natural resources in the People's Republic of China shall be under the jurisdiction of the people's courts of the People's Republic of China'.

In the author's opinion the jurisdiction provision in Civil Procedure Law is vague when referring to international contracts for the sale of goods. With emerging electronic contract disputes the Civil Procedure Law will appear to be increasingly insufficient. Although the Chinese Electronic Signature Law doesn't deal with any jurisdiction issues, China has tried to establish some regulations governing the internet with, for example, the Management of Chinese Computer Information Networks connected to International Networks Regulation,[92] as well as the Computer Information Network and Internet Security, Protection and Management Regulation.[93] These two regulations cover both civil and criminal issues. However, the rules relating to jurisdiction are still largely insufficient. There are specific rules to determine

which law should apply, such as Article 15 of the Management of Chinese Computer Information Networks Regulation which states vaguely that those who violate these regulations while at the same time breaking other relevant laws and administrative rules and regulations shall be punished in accordance with the relevant laws and administrative rules and regulations.

Overall, according to Chinese law, there are six basic principles to determine the jurisdiction: the domicile principle,[94] the personal jurisdiction principle,[95] the freedom of choice principle,[96] the principle of related location,[97] the exclusive jurisdiction principle[98] and the territorial jurisdiction principle.[99] The fundamental jurisdiction rule in Chinese conflict of laws is that a civil suit against a Chinese citizen comes under the jurisdiction of the court at the place where the defendant is domiciled or, if not the same, under the jurisdiction of the people's court at the place of his regular abode or residence.[100]

10.1.4 Summary: a comparative study

The EU and US both signed the Hague Convention on Choice of Court Agreements in 2009, which is considered an important step in the improvement of harmonisation of private international law. Compared to the EU special jurisdiction approach, the US specific jurisdiction approach is different. The Brussels I Regulation in the EU provides comprehensive rules on judicial co-operation between Member States, while the US adopts a market-oriented jurisdiction approach. For example, the US employs *Zippo*, 'effects' and 'targeting' tests determining internet jurisdiction, and the EU specifies classical general and special jurisdiction rules in the Brussels I Regulation.

Moreover, both the US and the EU have appeared to be applying their individually developed standards of determining jurisdiction in the context of conventional contracts to the jurisdictional problem of e-commerce. It may be necessary either to reform the law by modifying the normal rules on jurisdiction, or to reform the law by introducing a special regime of rules of jurisdiction for cases of electronic contracting. For the former, a new rule could be introduced into Article 5(1)(b) of the Brussels I Regulation, which would provide how to define the place of performance for digitised products and services. Some scholars have argued that this would be to treat electronic commerce contracts differently from other contracts, which goes against the current philosophy of Article 5(1).[101] In the author's view, to a broader respect, this would not be contrary to the fundamental principle that contracts can be formed by electronic means. But in a narrower view, electronic contracting or transactions do have their unique characters. However, the creation of a special regime of jurisdiction rules for e-commerce cases is a process which is time and money consuming. Even if efforts were made to draft a specific regulation or convention it would still take time and effort to come into force. It is conceivable that in future the new fast-developing

electronic communication industry will develop further techniques that would clearly indicate that existing laws were no longer suitable or applicable. A special regime of jurisdictional rules for electronic commerce would then be introduced on the ground that traditional territorially based concepts of jurisdiction were not entirely appropriate anymore to regulate cyberspace.

Compared with the EU and the US, China has a very similar approach, which comprises party autonomy, general jurisdiction and special jurisdiction. However, unlike the EU, China has no specialised comprehensive single law or regulation in the matter of jurisdiction. Such an instrument should be established in China in the future, learning from the experience of the EU and the US.

10.2 Applicable law for internet-related disputes

Applicable law (also called 'choice of law') is another issue within the regime of private international law or conflict of law. It means which law is chosen to resolve the dispute. Usually after deciding which court will hear the case (that is jurisdiction), the parties will need to be certain about which law will apply to the case. When parties make a choice of jurisdiction to hear the case, for example, the High Court of England, they usually intend to choose the corresponding law in that country, for example, English law, or vice versa. However, it is not absolute.

Regarding internet choice of law, the location and timing of contract negotiation and communication play an important role in the applicable law analysis for contracts. Generally, the location, where contracting occurs, provides the substantive law that governs the agreement under the rules of private international law; hence, the place of contracting determines the outcome. In determining the applicable law to online as opposed to offline commercial transactions the difference only arises when transactions involve digitised goods with electronic delivery.

10.2.1 EU

In the EU the EC Directive on Electronic Commerce does not include a choice of law provision but there is a 'country of origin' principle. It refers to the applicable law for service providers, stating that 'each Member State shall ensure that the information society services provided by a service provider established on its territory comply with the national provisions applicable in the Member State in question which fall within the coordinated field',[102] which relates to 'online activities', such as 'online information, online advertising, online shopping, and online contracting'.[103] The 'country of origin' principle aims to regulate the conduct of service providers in general, but not specifically contracting parties in electronic transactions. Thus, the 'country of origin' principle does not affect the application of the law chosen by the parties to govern a contract.[104]

One of the most important instruments regulating applicable law in the EU is the Rome Convention of 1980 (the Rome Convention).[105] It is an international agreement on uniform conflict of law rules in contract. According to Article 1 of the Rome Convention, the Rome Convention 'shall apply to contractual obligations in any situation involving a choice between the laws of different countries'. The Rome Convention specifies rules of applicable law in a clear structure. Firstly, Articles 3 and 4 are the core provisions of the Convention. Article 3 deals with the applicable law chosen by the parties while Article 4 contains the provisions for ascertaining the applicable law in the absence of choice. Secondly, there are provisions dealing with the mandatory rules of the forum (or of another country) or public policy. Thirdly, choice of law rules apply to specific aspects of a contract, such as material and formal validity, interpretation, performance and the quantification of contractual damages.

In the early 2000s, the European Economic and Social Committee and the European Parliament were in favour of converting the Rome Convention of 1980 into a Community Regulation and modernising certain provisions of the Rome Convention, making them clearer and more precise. The proposal for a 'Regulation of the European Parliament and the Council on the Law Applicable to Contractual Obligations (Rome I)',[106] was finally adopted by the Commission on 15 December 2005 in Brussels. The Vice-President said: 'By providing foreseeable and simplified rules, the Rome I proposal on the law applicable to contracts will enable Europe's citizens and firms to make more of the possibilities offered by the internal market'.[107]

On 17 June 2008 the European Commission adopted the Regulation of the European Parliament and the Council on the law applicable to contractual obligations (Rome I).[108] The Rome I Regulation replaced the Rome Convention in Member States except for those Member States that fall within the territorial scope of the Rome Convention and to which Rome I does not apply by virtue of Article 299 of the EC Treaty.[109] Rome I shall apply to contracts concluded after 17 December 2009.[110]

The Rome I Regulation intends to establish consistency with the Brussels I Regulation with regard to the relationship between jurisdiction and choice of law. As provided by Recital 7 of the Rome I Regulation, 'the substantive scope and the provisions of this Regulation should be consistent with Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters[111] (Brussels I)'.

The Rome I Regulation, just like the Rome Convention, does not specifically deal with electronic commercial transactions. However, it provides the provisions relating to the choice of law rules for reference in online contracting. Just as in normal contracts, contracts made via electronic communications may also insert a choice of law agreement/clause. In the absence of a choice of law clause it will be even more difficult to determine applicable law than for normal contracts due to the unique features of electronic communications.

The modernisation and radical reform of Article 3 on choice by the parties of the applicable law, Article 4 concerning determination of the applicable law in the absence of choice and Article 5 on consumer contracts,[112] may make it clearer and easier to ascertain the applicable law for an e-contract than the Rome Convention.

The applicable law in cases of choice

Article 3 of the Rome I Regulation attempts to strengthen the freedom of parties in the business world to choose the applicable law. Article 3(1) and (2) of the Rome I Regulation have slightly changed the wording but retained the same meaning as that of the Rome Convention. Article 3(3) and (4) of the Rome I Regulation replace Article 3(3) of the Rome Convention, providing more comprehensive rules on parties' freedom of choice of law. Article 3(3) and (4) enhance the provision that the chosen law should govern the law rather than the law of the country that has more factual links unless it cannot be derogated from by agreement according to a relevant rule.

Article 3(1) is a fundamental rule providing party autonomy in choice of law that 'a contract shall be governed by the law chosen by the parties. The choice shall be made expressly or clearly demonstrated by the terms of the contract or the circumstances of the case. By their choice the parties can select the law applicable to the whole or to part only of the contract'. Contracts frequently contain different obligations, so the parties must have freedom of subjecting the different obligations to different laws. That is known as 'splitting the applicable law'.[113] This may be divided into four different categories: first, it is possible to apply different laws to different aspects of the same obligation; secondly, different terms of one contract may be governed by different laws;[114] thirdly, different groups of obligations may be governed by different laws;[115] fourthly, the obligations of each party may be governed by a different law.[116]

Moreover, parties must have freedom to re-choose their chosen law. Article 3(2) further clarifies that the previous choice of law can be changed by the agreement of the parties after the conclusion of the contract. By virtue of this provision, the parties may, having included a choice of law clause in their contract, subsequently decide to change the applicable law by a new mutual agreement. Alternatively, in a situation where the contract does not include a choice of law, the parties may agree on the applicable law at some later stage. If parties are free to decide on the applicable law, there is no reason why they should not be able to change it.[117]

In the author's opinion, the recognition of electronic means adopted by the Choice of Court Convention should also be used in Choice of Law. The rules concerning the choice of law in the online world can best be explained by the most recent international legislation: the UN Convention on the Use of Electronic Communications in International Contracts (the UN Convention). In the electronic commerce environment parties have the same freedom

to include a choice of law clause when concluding contracts online because the UN Convention explicitly employs 'party autonomy' in the choice of a party's place of business. Thus, party autonomy is the core principle of the UN Convention. Furthermore, parties can amend their choice of law clause. The new choice of law clause that parties agree will not affect the validity of the contract. The provision of 'error in electronic communications'[118] in the UN Convention supports the above principle. It provides that the information system should provide the other party with an opportunity to correct the input error. Thus, parties might have an opportunity to add or amend a choice of law clause in the 'addition information' or 'comments' space box on the website, or they might enclose or upload a document expressing the intention to change the applicable law, or they might put forward another email followed by their transaction noticing the amendment of the applicable law. However, that, which party's proposal prevails, also depends on the rules of battle of forms previously discussed in Part II.

Applicable law in the absence of choice

With regard to the applicable law in the absence of choice, according to Article 4(1) of the Rome Convention, the law of the country where it is most closely connected governs the contract. The closest connection is a vague formula because it leaves it to the courts to weigh up the factors that determine the 'centre of gravity' of the contract.[119] To consolidate certainty Article 4(2) of the Rome Convention establishes a general presumption that 'the contract is most closely connected with the country where the party who is to effect the performance which is characteristic of the contract has, at the time of conclusion of the contract, his habitual residence'. The Rome I Regulation deleted Article 4(1) of the Rome Convention, replacing it with more precise rules whose 'proposed changes seek to enhance certainty as to the law by converting mere presumptions into fixed rules and abolishing the exception clause'.[120] For a contract of sale or the provision of services the Rome I Regulation has reserved the rule in the Rome Convention whereby the applicable law is the law of the place where the party performing the service characterising the contract has his habitual residence.[121] It provides that 'a contract of sale shall be governed by the law of the country in which the seller has his habitual residence'.[122] Where characteristic service of the contract cannot be identified the contract 'shall be governed by the law of the country where it is most closely connected'.[123]

As illustrated above, Article 4 of the Rome I Regulation aims to specify the rules applicable, in the absence of a choice, as precisely and foreseeably as possible so that the parties can decide whether or not to exercise their choice. To assist the application of Article 4, the Proposal also inserted a new provision of the interpretation of 'habitual residence' under Article 19, which is identical to Article 4(2) of the Rome Convention. Article 19(1) of the Rome I Regulation provides that the principal establishment of companies shall be

considered to be the habitual residence, or the habitual residence will be deemed to be the one of a subsidiary/branch, if the contract was made in the course of operation or performance that was the responsibility of that subsidiary/branch. The difference from the Rome Convention is that Article 19(2) of the Rome I Regulation provides that 'where the contract is concluded in the course of the operations of a branch, agency or any other establishment, or if, under the contract, performance is the responsibility of such a branch, agency or establishment, the place where the branch, agency or any other establishment is located shall be treated as the place of habitual residence', whilst Article 4(2) of the Rome Convention would determine it as the principal place of business.

With regard to requirements as to form, however, the Proposal did not expressly set out the 'function equivalent' rule for electronic mails. The International Chamber of Commerce (ICC) and the UK Government responded to the Green Paper on the conversion of the Rome Convention into a Community instrument[124] (hereafter Green Paper) on whether Article 9 of the Rome Convention[125] should be reformed. According to the opinion of the ICC and the UK, Article 9 adequately covered contracts concluded by email; thus, there should be no need to modify this article.[126] A contract concluded by email in the same country or different countries shall be valid if it satisfies the formal requirements of the law of either of those countries. Moreover, the Green Paper advises that 'as regards contracts concluded at a distance (by fax, mail or email, for example), there is a place of conclusion for each party in the contract, which further multiplies the chances that the contract is valid as to form. This solution has made it unnecessary to take a more or less artificial decision on the location of a contract between distant parties'.[127]

In the author's view, Article 9 of the Rome Convention was drawn up before electronic contracts came into common practice; thus, the determination of the place of conclusion is different from that of offline. According to the UN Convention on the Use of Electronic Communications in International Contracts, the place of dispatch or receipt of an electronic communication is the place where the party has its place of business,[128] but if the party does not have a place of business, reference should be made to his habitual residence.[129] It might be advisable for Article 9 of the Rome Convention to contain an additional rule by adding the law of the country where either of the parties has its habitual residence. It would thus constitute three laws for formal requirements as to form: the law which governs it under this Regulation; the law of the country of the place of conclusion; and the law of either party's habitual residence.[130]

The Commission of the European Communities amended Article 9 of the Rome Convention in Article 10 of the Proposal for a Regulation of the European Parliament and the Council on the law applicable to contractual obligations (Rome I),[131] adding 'habitual residence' as a linking factor. Article 10 of the proposal is adopted in Article 11 of the Rome I Regulation, which is more accurate but without substantially changing the content. It provides that:

1. A contract concluded between persons who, or whose agents, are in the same country at the time of its conclusion is formally valid if it satisfies the formal requirements of the law which governs it in substance under this Regulation or of the law of the country where it is concluded.
2. A contract concluded between persons who, or whose agents, are in different countries at the time of its conclusion is formally valid if it satisfies the formal requirements of the law which governs it in substance under this Regulation, or of the law of either of the countries where either of the parties or their agent is present at the time of conclusion, or of the law of the country where either of the parties had his habitual residence at that time.
3. A unilateral act intended to have legal effect relating to an existing or contemplated contract is formally valid if it satisfies the formal requirements of the law which governs or would govern the contract in substance under this Regulation, or of the law of the country where the act was done, or of the law of the country where the person by whom it was done had his habitual residence at that time.[132]

In the author's opinion, a subsidiary rule concerning the validity of electronic communications should also be addressed in Article 11 of the Rome I Regulation – that a choice of law clause shall be valid both in writing and by electronic means. Employing a provision from Article 3(c) of the Choice of Court Convention, it can be proposed that:

A choice of law agreement can be concluded or documented:

1) in writing; or
2) by any other means of communication which renders information accessible so as to be usable for subsequent reference;[133]

With regard to applicable law in electronic contracts determining the applicable law in absence of choice is a two-stage exercise: firstly, the seller's habitual residence needs to be ascertained; secondly, if the seller's habitual residence cannot be determined, the court will identify the characteristic performance of the contract, the country of the party who is to effect it and determine the law which is most closely connected to the contract. Compared to the Rome Convention, which starts with the close connection principle, the Rome I Regulation explicitly expresses that 'the contract shall be governed by the law of the country in which the seller has his habitual residence'.[134] With regard to consumer contracts, Article 6 of the Rome I Regulation clearly provides that 'a contract shall be governed by the law of the country where the consumer has his habitual residence'. Overall the Rome I Regulation is more precise for parties to determine the applicable law in both B2B and B2C commercial matters.

10.2.2 US

Unlike the EU, the US has a special provision governing choice of law in the Uniform Computer Transactions Act (UCITA). Although UCITA only applies to computer information transactions such as computer software, online databases, software access contracts or e-books[135] involving licensing contracts, the choice of law provision of UCITA can be learned or adopted in general electronic contracting for the reason that the feature of concluding contracts with transferring products online will be identical to that of transacting computer information. Without a uniform piece of the US Private International Law, traditional uniform commercial laws, such as the Uniform Commercial Code (UCC) and the Second Restatement, have to be employed to determine applicable law to contracts concluded and performed electronically.

Similar to the EU there are two core doctrines in ascertaining applicable law: freedom of choice and absence of choice. Freedom of choice, so-called 'party autonomy', is the fundamental rule. It means that the parties are free to select the law governing their contract, subject to certain limitations.[136] Party autonomy is recognised by §109(a) of UCITA, §187 of the Second Restatement as well as by §1–105 of the Uniform Commercial Code.[137] In the absence of parties' choice, §109 of UCITA and §188 of the Second Restatement deal with it.

The applicable law in cases of choice

With regard to the applicable law in cases of choice, §1–105 of the Uniform Commercial Code provides that 'the parties may agree that the law either of this state or of such other state or nation shall govern their rights and duties'. The Second Restatement, §187(1) also provides that 'The law of the state chosen by the parties to govern their contractual rights and duties will be applied if the particular issue is one which the parties could have resolved by an explicit provision in their agreement directed to that issue'. The Second Restatement, §187(2) further requires that the party's choice should have a close relationship either to them or to the transaction, or there should be a 'reasonable basis', and not be contrary to 'a fundamental policy of a state'.[138] The UCITA expressly deals with choice of law issues. UCITA, §109(a) states that 'parties in their agreement may choose the applicable law', but such choices are not enforced if they are determined to be unconscionable.[139] Under §105(b), a court will also refuse to recognise the chosen law if it violates the fundamental public policy of the forum state.

As illustrated above, it is similar to the Rome I Regulation in the EU that the US laws favour and respect the election of the applicable law by contracting parties. However, the limitation of freedom of choice in the EU and US is different in two aspects: firstly the US requires that the state of the choice of law must have a substantial relationship to the parties or

transactions with a reasonable basis, whilst the EU does not require for the chosen law to have any real connection with the parties or the subject matter of their contract;[140] secondly, in the US the Second Restatement excludes the choice of law if it contradicts the 'fundamental policy' of the state whose law would be applicable to the contract in the absence of any choice by the parties, whilst in the EU, the Rome Convention prevents the parties opting out of the mandatory rule. To illustrate the 'mandatory rules' of the Rome Convention, if contracting parties A and B choose the law of Country B as their governing law, but the law of Country A contains mandatory rules, the mandatory rules of Country A will override any different rule in the law of Country B.

The basic methodology in choice of law is to characterise the issue or question to fit into a category, to determine the connecting factor for that category, and then to apply the law indicated by that connecting factor.[141] Many disputes involving e-commerce arise between parties who are bound by a contract that specifies the terms and conditions upon which they have agreed to interact. Frequently the contract itself may provide that any dispute arising from it is to be heard in the courts of a specified state (i.e. choice of forum or forum selection clause) and is to be determined under the substantive laws of a specified state (i.e. choice of law clause).[142] Generally, contracting parties will choose the applicable law on the basis of the place of contract formation, the place of performance, domicile or the state of incorporation, corporate headquarters and branches.

It may be difficult to determine whether the parties have genuinely consented to a choice of a particular law which appears as a standard term on the seller's website and which might not be immediately visible to the buyer. It becomes therefore a primary concern that a choice-of-law clause contained on an internet site, or included in an email, was sufficiently visible and actually represents the bilateral consent of the parties. Take a clickwrap agreement as an example: a choice of law clause is included by the seller on his website but is not directly visible on screen and can only be seen when scrolling down the screen or clicking on a separate link. The seller alleges that the buyer consents to the clause when he concludes the contract, even though he never properly reads that clause. So can it be deemed to be lack of parties' consent? If the seller performs his duty of making a contract available online,[143] that is, the buyer can get back to the terms and conditions on the website any time he wants (even after the contract is concluded), then it will be the buyer's responsibility to make sure of the choice of law clause before he clicks the 'I agree' button. Once clicking the 'I agree' button, the parties will be deemed to have consented to the terms and conditions.

The applicable law in absence of choice

The Uniform Commercial Code, §1–105 provides that in absence of a choice of law agreement 'this Act applies to transactions bearing an appropriate

relation to this state'. Under §188 of the Second Restatement, where a choice of law provision is absent from a contract, the court has to determine whether to apply the substantive laws of one state over another in resolving the issues presented before it. The Second Restatement, §188(1) determines the applicable law in absence of effective choice by the parties, providing that 'The rights and duties of the parties with respect to an issue in contract are determined by the local law of the state which, with respect to that issue, has the most significant relationship to the transaction and the parties under the principles stated in §6'.[144] The Second Restatement, §188(2) further provides the connecting factors in determining the applicable law in the absence of choice, including '(a) the place of contracting, (b) the place of negotiation of the contract, (c) the place of performance, (d) the location of the subject matter of the contract, and (e) the domicile, residence, nationality, place of incorporation and place of business of the parties. These contacts are to be evaluated according to their relative importance with respect to the particular issue'. According to §188(3) the local law of this state will usually be applied, if the place of negotiating the contract and the place of performance are in the same state.[145]

Furthermore, both the Second Restatement, in §191, and the Uniform Commercial Code (UCC), in §1–105(1) in combination with §2–401, deal with the sale of goods. The Restatement provides, subject to the usual exception in favour of an express choice by the parties or a more significantly related law, that the law of the place should be applied 'where under the items of the contract the seller is to deliver the chattel'. The UCC, §1–105(1) provides for the application of forum law whenever the transaction bears an 'appropriate relation' to the forum.[146]

However, while §188 governs contracts of sale for both goods and services, §191 specifically regulates the sale of goods, §204 provides, for all contracts, that a contract should be construed under the law generally applicable under §188 (the place of the most significant relationship) and §191 provides a reference to the place of delivery that the:

> validity of a contract for the sale of an interest in a chattel and the rights created thereby are determined, in the absence of an effective choice of law by the parties, by the local law of the state where under the terms of the contract the seller is to deliver the chattel unless, with respect to the particular issue, some other state has a more significant relationship under the principles stated in §6 to the transaction and the parties, in which event the local law of the other state will be applied.

However, the case law largely ignores the Second Restatement provisions and refers questions of construction either to the contract's 'centre of gravity',[147] or the law of the place of making,[148] whereby the two often coincide on the facts of a given case.[149]

With regard to digitised goods and services, §109(b)(3) of the UCITA

provides that 'In the absence of an enforceable agreement on choice of law, the following rules determine which jurisdiction's law governs in all respects for purposes of contract law: the contract is governed by the law of the jurisdiction having *the most significant relationship* to the transaction', while §109(b)(1) and (2) specifically refers to the location of the licensor in an access contract and the location of the physical delivery in a consumer contract.[150] In the author's view the action and nature of a licensor who transfers computer information and electronically delivers a copy of software containing information, is identical to that of a seller concluding a contract online with electronic delivery of goods. Thus, if the law of the place where the licensor is located governs the applicable law, then it can be presumed that the law of the place where the seller is located should govern the applicable law. In this case where a party is located should be understood as where he has a place of business.[151]

Under the UCITA, in the absence of an applicable choice-of-law provision, the law of a foreign jurisdiction will apply only if it provides substantially similar protections and rights to a party located in a domestic jurisdiction.[152] §109(d) further provides that 'a party is located at its place of business if it has one place of business, at its chief executive office if it has more than one place of business, or at its place of incorporation or primary registration if it does not have a physical place of business. Otherwise, a party is located at its primary residence'.

As illustrated above 'the most significant relationship to the transaction' is a connecting factor to determine the applicable law in the absence of choice both online and offline. The 'most significant relationship' test requires consideration of factors including:

> place of contracting; place of negotiation; place of performance; location of the subject matter of the contract; domicile, residence, nationality, place of incorporation and place of business of one or both parties; needs of the interstate and international systems; relative interests of the forum and other interested states in the determination of the particular issue; protection of justified and other interested states in the determination of the particular issue; protection of justified expectations of the parties; and promotion of certainty, predictability and uniformity of result.[153]

However, the 'place of contracting' appears to be the weakest basis for party autonomy; such a contract is easy to manipulate and may result in an 'interstate contract', that is a contract that becomes valid by virtue of the interstate factor although it would be defective in any state with a more real connection. With regard to 'place of performance', for instance, if the seller A sold the software to the buyer B in the US and installed it in London, under these circumstances, where was the contract performed? It is hard to determine. It should be suggested that the instalment agreement alongside the sales of

goods contract is deemed to be the secondary agreement, thus the place of performance is regarded to be the place of performance of the main contract – that is, in the US.

To summarise, in the US the contract will be governed by the law of the country where it has the most significant relationship to the contract, which is identical to the closest connection principle in the EU. Furthermore the law where the licensor is located, which is at his place of business, will govern the contract under Article 109 of UCITA. According to the findings in the applicable law in B2B electronic contracts, the place that has the most significant relationship to the contract or transaction would be the seller's place of business. Thus, the law of the country that has the closest relationship to electronic contracts or transactions should be the law of the seller's place of business, which is compatible with the Rome I Regulation.

10.2.3 China

In China the two general principles to determine applicable law in contracts are the same as those in the EU and US: first is party autonomy that parties are free to choose the applicable law governing the contract; second, the closest connection or the most significant relationship to the contract or transaction is regarded as a linking factor to determine the applicable law in absence of choice. However, China is a civil law country with written laws. There would be no choice of law contracting matters in China unless the contract includes an 'international' factor.[154] A contract is deemed to be 'international' when (a) at least one party is not a Chinese citizen or legal person, (b) the subject matter of the contract is in a third country (i.e. the goods to be sold or purchased are located outside of China), or (c) the conclusion or performance of the contract is made in a third country.[155]

Party autonomy/freedom of choice

With regard to applicable law in foreign contracts, the National People's Congress of the People's Republic of China enacted a unified Contract Law,[156] which has been in force since 1 October 1999. Article 126 of the Chinese Contract Law provides that 'Parties to a foreign related contract may select the applicable law for resolution of a contractual dispute, except otherwise provided by law'.[157] Furthermore, Chapter VIII of General Principles of Civil Law of P.R. China[158] determines which applicable law should be applied in civil relations with foreigners. Article 145 of the General Principle of Civil Law provides that 'the parties to a contract involving foreign interests may choose the law applicable to settlement of their contractual disputes, except as otherwise stipulated by law'.

Applicable law in absence of choice

To determine applicable law in absence of choice, Article 126 of the Chinese Contract Law provides that 'If the parties to a contract involving foreign interests have not made a choice, the law of the country to which the contract is most closely connected shall be applied'.[159] It then further tackles specific points, such as 'the contracts for Chinese-foreign equity joint ventures, Chinese-foreign contractual joint ventures and Chinese-foreign cooperative exploration and development of natural resources to be performed within the territory of the People's Republic of China shall apply the laws of the People's Republic of China'.[160] Article 145 of the General Principle of Civil Law also provides that 'the parties to a contract involving foreign interests may choose the law applicable to settlement of their contractual disputes, except as otherwise stipulated by law; If the parties to contract involving foreign interests have not made a choice, the law of the country to which the contract is most closely connected shall be applied'.

The Supreme Court of China has accepted the idea of applying characteristic performance in order to achieve a more efficient determination of the applicable law under the 'closest connection' rule. It decided to make it one of the standards used to judicially determine the applicable law. The reason for the Supreme Court's adoption of the characteristic performance based criteria is twofold: firstly, it makes the determination more objective by limiting the discretionary powers of the courts when determining the applicable law. Secondly, this approach will improve the result's certainty, predictability and uniformity.[161]

The Supreme Court explains the characteristic performance that in a contract for the international sale of goods the law that is most closely connected with the contract is the law of the seller's place of business at the conclusion of the contract. If, however, the contract was negotiated and concluded in the place of the buyer's business, the applicable law shall then be that of the place of the buyer's business.[162] A foreign law cannot be chosen as the applicable law if it violates the social public order of China. At the time of concluding contracts in international sale of goods online, the seller may sit at his place of business, communicating electronically with the buyer who may sit at his place of business. The electronic contract will then be without the seller and buyer's physical presence. Thus, the Chinese Supreme Court's rationale is not applicable to electronic contracting. In an electronic contract the applicable law is the law of the seller's place of business before or at the conclusion of the contract. In short, 'party autonomy' is the principle of ascertaining the applicable law, whereas 'closest connection', the same as the EU and US, is the factor to determine the applicable law in absence of choices. The closest connection to the contract concluded online should be the seller's place of business, if not his habitual residence.

10.2.4 Summary: a comparative study

The EU, US and Chinese choice of law systems are all in favour of party autonomy. The parties are free to choose the governing law and state it in the contract (in cases of express choice or its equivalent). Otherwise the contract will be governed by the law of the country with which the contract is most closely connected or has the most significant relationship to the transaction in cases of absence of express choice. In the author's opinion the place of business and the place of performance are more difficult to determine in electronic transactions. Generally, traditional choice of law principles should still apply to electronic contracts if the delivery of goods involves physical transfer. However, due to the complex and unique nature of online contracting when involving electronic delivery it is necessary to further establish or clarify the methods of determining the applicable law to e-contract disputes. For instance, in the absence of a choice of law clause in electronic contracts, how do we ascertain the 'most closely connected' factor over the internet in order to determine the applicable law?

In the absence of choice of law the law of the country which is most closely connected with the contract will govern the contract. This will be determined by looking at the most closely connected factors: where is the place of performance and do the defendant's activities have effects in that state? According to the findings in the EU, US and China, the seller's place of business seems to be the most enduring connecting factor, which has the economic impact on its area, thus the law of the seller's place of business should be the law governing B2B electronic contracts in the absence of a choice of law clause.

10.3 Online dispute resolution

In the 1980s, alternative dispute resolutions (ADR) were most commonly used to resolve international commercial transactions disputes rather than cross-border litigation. ADR, including arbitration, mediation/conciliation and negotiation, is considered more efficient, flexible, confidential and less costly, compared with traditional litigation. ADR can avoid the long court proceedings for international disputes which are affected by the conflicts of jurisdiction and choice of law. International instruments have been developed to promote the harmonisation of international ADR practices, such as the 1958 New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards; the UNCITRAL Model Law on International Commercial Arbitration 1985 and the UNCITRAL Model Law on International Commercial Conciliation 2002.

In the early 1990s global internet transactions or usages increased the probability of cross-border disputes. Parties situated in different continents may be opposed over small claims or cyber-related issues. These kinds of disputes challenge the traditional dispute resolutions because:

1) Different countries have different rules for trade and various prohibitive costs of legal action across jurisdictional boundaries;
2) Much less obvious localisation factors on the internet cause difficulties in determining the place of business or the place of performance in cyberspace due to the boundless internet that may be accessed from anywhere in the world;
3) Cyber-related disputes may require a legal expert who is equipped to adapt to the diverse evolving technological, social nature and commercial practice of cyberspace.

So what will be the least costly but most efficient solution to resolve e-disputes?

The modernisation of ADR – online dispute resolutions (ODR) – was introduced in the mid-1990s by the Virtual Magistrate at Villanova University, the Online Ombuds Office at the University of Massachusetts, the Online Mediation Project at the University of Maryland, and the Cyber-Tribunal Project at the University of Montreal, Canada.[163] It aims to provide more efficient, cost effective and flexible dispute resolutions in the information society. ODR takes advantage of this, a resource that extends what we can do, where we can do it, and when we can do it.[164] The ABA Task Force on E-Commerce and ADR provides a generic definition of ODR:

> ODR is a broad term that encompasses many forms of ADR and court proceedings that incorporate the use of the internet, websites, email communications, streaming media and other information technology as part of the dispute resolution process. Parties may never meet face to face when participating in ODR. Rather, they might communicate solely online.[165]

As defined in the ABA Task Force, ODR is also an extension of ADR – online arbitration, online mediation and online negotiation – as well as an application of cybercourts, although online litigation is not as common as eADR.

10.3.1 Current legislation in the EU, US and China

EU

In the EU, ADR (in particular arbitration and mediation) use is encouraged to resolve cross-border commercial disputes. The importance of arbitration in the community is highlighted in the Commission's Report on the Review of the Brussels I Regulation on 21 April 2009 – that the Brussels I Regulation has in specific instances been interpreted so as to support arbitration and the recognition/enforcement of arbitral awards.[166] The Green Paper that accompanies this Report further explains, 'however, addressing certain specific

points relating to arbitration in the Regulation, not for the sake of regulating arbitration, but in the first place to ensure the smooth circulation of judgments in Europe and prevent parallel proceedings'.[167]

Another common method of ADR, mediation, is also encouraged by the community in resolving civil and commercial matters. The EC Directive of the European Parliament and of the Council on Certain Aspects of Mediation in Civil and Commercial Matters (hereafter EC Directive on Mediation) was approved by the European Parliament on 23 April 2008[168] and entered into force in June 2008.[169] The purpose of the EC Directive on Mediation is to facilitate access to dispute resolution, to encourage the use of mediation, and to ensure a sound relationship between mediation and judicial proceedings.[170] It is considered to be an achievement of regulating out-of-court dispute resolutions. It is in favour of electronic communications and, to an extent, online dispute resolution. It encourages the use of mediation in cross-border disputes and the use of modern communication technologies in the mediation process, which is reflected by Recitals (8) and (9) of the Mediation Directive:[171]

> (8) The provisions of this Directive should apply only to mediation in *cross-border* disputes, but nothing should prevent Member States from applying such provisions also to internal mediation processes.
> (9) This Directive should not in any way prevent the use of *modern communication technologies* in the mediation.[172]

Moreover, the provisions of 'ensuring the quality of mediation'[173] and 'information for the general public'[174] also indicate the support of using ODR in the EU. For example, Article 4 of the EC Directive on Mediation encourages Member States 'by any means which they consider appropriate' to develop voluntary codes of conduct mediation services, as well as other effective quality control mechanisms. In addition, Article 9 of the EC Directive on Mediation explicitly encourages Member States to make service and contact information available to the general public 'by any means which they consider appropriate in particular on the Internet'.

In general, although there are no substantial ODR rules in the EC Directive on Electronic Commerce, it encourages ODR practice by requiring Member States to ensure that their legislation 'does not hamper the use of out-of-court schemes, available under national law, for dispute settlement, including appropriate electronic means'.[175] In addition, it requires Member States to 'encourage bodies, responsible for the out-of-court settlement of, in particular, consumer disputes to operate in a way which provides adequate procedural guarantees for the parties concerned'[176] and to 'encourage bodies responsible for out-of-court dispute settlement to inform the Commission of the significant decision they take regarding Information Society services and to transmit any other information on the practices, usages, or customs relating to electronic commerce'.[177]

US

In the US there is no uniform legislation regulating ODR services. Self-regulation and adoption of best practice guidelines are the approaches recommended by the American Bar Association (ABA).[178] In 2002 the ABA Task Force on Electronic Commerce and Alternative Dispute Resolution final recommendations and report on disputes in electronic commerce emphasised that an ODR transaction is 'an e-commerce transaction in and of itself'. The ABA essentially recommends best practice principles that ODR providers should adhere to, such as adequate standards and codes of conduct and the achievement of transparency through information and disclosure as a basis to attain sustainability.[179] A non-profit, educational and informational entity, iADR Centre, is also recommended by the Task Force.

The US self-regulation arbitration and mediation module rules from the American Bar Association (ABA) and American Arbitration Association (AAA) are most widely used in US ADR practices. In September 2005 the ABA adopted the Model Standards of Conduct for Mediators[180] which specified nine standards of conduct for mediators – they are: self-determination, impartiality, conflicts of interest, competence, confidentiality, quality of the process, advertising and solicitation, fees and charges, as well as advancement of mediation practice. The AAA also promulgated Commercial Arbitration Rules and Mediation Procedures in 1999.

China

In China, on 31 August 1994, the Arbitration Law was promulgated by the Chinese National People's Congress with the aim of establishing a coherent nationwide arbitral system, entering into force on 1 September 1995. The establishment of online arbitration is subject to the restrictions and requirements due to different local market entries in different provinces in terms of registration,[181] conditions for arbitrators' appointment,[182] and requirements of establishment.[183] To harmonise the standard of online arbitration practice in China, China International Economic and Trade Arbitration Commission (CIETAC) promulgated 'Online Arbitration Rules' on 8 January 2009, which came into force on 1 May 2009. These Rules are formulated to arbitrate online contractual and non-contractual economic and trade disputes and other such disputes. The CIETAC Online Arbitration Rules apply to resolution of disputes over electronic commerce transactions, and other economic and trade disputes in which the parties agree to apply these Rules for dispute resolution.[184] The CIETAC has provided successful online arbitration services on .CN domain name disputes since 2002, which offers an ODR pioneer experience in China. The launch of the CIETAC online arbitration rules can be deemed to be one of the outcomes of the harvest of CIETAC ODR experience, and it will facilitate the development of online dispute resolution in China.

Mediation, different from arbitration, is used to resolve commercial dispute resolution to maintain ongoing business relationships.[185] The Chinese legislation is supportive of mediation in civil and commercial disputes. For example, Article 51 of the Civil Procedure Law of the People's Republic of China[186] permits the parties to 'reach a compromise of their own consent'. Article 49 of the Arbitration Law of the People's Republic of China[187] stipulates that parties may reach a private settlement even after the commencement of arbitration proceedings. Article 25 of the Law of the People's Republic of China on Chinese-foreign Contractual Joint Ventures[188] also provides that: 'Any dispute between the Chinese and foreign parties arising from the execution of the contract or the articles of the association for a contractual joint venture shall be settled through consultation or mediation'.

There are not many ADR international instruments that China, the US and the EU all agree on, but China, the US and most of the countries in the EU including the UK have signed and ratified the 1958 Convention on the Recognition and Enforcement of Foreign Arbitral Awards (hereafter the New York Convention).[189] The New York Convention is considered to be one of the most successful conventions, which gives the certainty of recognition and enforcement of a cross-border arbitral award. As the New York Convention was adopted long before the birth of the electronic communication society it did not include the function equivalent rule to recognise the validity of electronic arbitration agreements and awards. According to Article 2(1) of the New York Convention each contracting state shall recognise an agreement in writing. Online arbitration has been challenged as to whether the electronic arbitration agreements and awards can meet the requirements on the written form under the New York Convention. It is suggested that if the digital arbitral awards can be printed and signed, it would satisfy the written requirement. However, if electronic arbitration agreements and arbitral awards can be treated as 'electronic contracts' their validity will be automatically recognised by the UN Convention on the Use of Electronic Communications in International Contracts and other national electronic contract laws.

10.3.2 Global successful examples of ODR services

In the author's view, up until 2009, the most successful ODR services in the world are:

1 eBay and SquareTrade;
2 AAA (the American Arbitration Association) and Cybersettle;
3 ICANN (the Internet Corporation for Assigned Names and Numbers) and WIPO-UDRP (the World Intellectual Property Organization – Domain Name Dispute Resolution Policy);
4 CIETAC (China International Economic and Trade Arbitration Commission); and HKIAC (Hong Kong International Arbitration Centre).

eBay and SquareTrade

eBay is one of the world's largest online marketplaces providing trading platforms and was established in 1995. SquareTrade is an industry-leader in online merchant verification and dispute resolution, created in 1999. Both eBay and SquareTrade are independent private companies. Although they are engaged in different internet industries they have a common aim of promoting customers' confidence in doing business or using services online.

This aim is reflected in eBay e-trust strategies. The eBay e-trust strategies are designed to make customers comfortable with buying and selling online so that a maximum number of sellers and buyers will be attracted to its online marketplace. The trust building measures of eBay include: 1) the mutual rating system of trade satisfaction; 2) identity verification; 3) secure online payment services like PayPal or Escrow; 4) insurance policy; and 5) last but not least the online dispute resolution (ODR) service provided by SquareTrade.

SquareTrade, eBay's preferred dispute resolution provider, helps eBay users who have disputes in eBay transactions. SquareTrade's position is practically that of an in-house dispute resolution provider as eBay refers its users exclusively to SquareTrade through a link on its website. There are two stages in the general operation of the eBay–SquareTrade system. At the first stage SquareTrade offers eBay users a free web-based forum which allows users to attempt to resolve their differences on their own. It is known as an 'automated negotiation platform'. When settlement cannot be reached at the first stage SquareTrade offers the use of a professional mediator with a nominal sum of fees as eBay will subsidise the rest of the cost.[190] This second stage is called 'online mediation'.

The usage of SquareTrade by eBay will be of benefit in resolving misunderstandings fairly, providing a neutral go-between for buyers and sellers, reducing premature negative feedback and generating trust in the eBay community.[191]

AAA and Cybersettle

The American Arbitration Association (AAA), established in 1926, is a non-profit making public service organisation and a global leader in conflict management, providing services to individuals and organisations who wish to resolve conflicts out of court. It also serves as a centre for education and training, issues specialised publications and conducts relevant research.[192] Cybersettle, founded in the mid 1990s, is a pioneer in online negotiation and an inventor and patent-holder of the online double-blind bid system. Both AAA and Cybersettle have their profound reputation and exclusive merits in their fields.

On 2 October 2006 AAA and Cybersettle announced a strategic alliance that will provide clients of both companies with the opportunity to use the

dispute resolution services of both companies exclusively – the goal is 'ensuring that no one walks away without a resolution' said Cybersettle President and CEO Charles Brofman. AAA clients using the AAA's online case management tools will be able to attempt settlement with Cybersettle before AAA neutrals are selected. Cybersettle clients who have not been able to reach settlement through online negotiation will be able to switch to the AAA's dispute resolution processes, including conciliation, mediation and arbitration.[193]

This strategic alliance not only makes full use of the reputation and merits of both parties, but also takes advantage of their different successful experiences. For example, AAA offers a broad range of dispute resolution services to business executives, attorneys, individuals, trade associations, unions, management, consumers, families, communities, and all levels of government, while since 1996 Cybersettle has handled more than 162,000 transactions, with more than $1.2 billion in settlements.[194]

AAA, an experienced public sector entity, cooperates with Cybersettle, a young enthusiastic private sector entity, which can be a model or a good strategic plan for the development of the ODR industry. Professional regulations of AAA, such as Commercial Arbitration Rules and Mediation Procedures, can be integrated into the self-regulation of private ODR services, which enhance the standardisation of the ODR order in society. AAA's dispute resolutions rules are professional and comprehensive, and contain Procedures for Large, Complex Commercial Disputes, as well as Supplementary Rules for the Resolution of Patent Disputes and a Practical Guide on Drafting Dispute Resolution Clauses, including negotiation, mediation, arbitration and large, complex cases. On the other hand Cybersettle can also contribute its private practices and work with AAA to promote other services when appropriate and to make joint proposals and business presentations under certain circumstances.

ICANN and WIPO-UDRP

The Internet Corporation of Assigned Names and Numbers (ICANN) and the World Intellectual Property Organization (WIPO) are both public international organisations but with different functions. ICANN is responsible for managing the generic top level domains in urgent need of a solution to a dispute resolution problem,[195] while WIPO is responsible for developing a balanced and accessible international intellectual property (IP) system.[196] In 1994 the WIPO Arbitration and Mediation Centre was established to provide ADR services – arbitration and mediation for the resolution of international commercial disputes between private parties. Its WIPO Electronic Case Facility (WIPO ECAF) has been designed to offer time and cost-efficient arbitration and mediation in cross-border dispute settlements.[197]

ICANN adopted the Uniform Domain Name Dispute Resolution Policy

(UDRP), which came into effect on 1 December 1999, for all ICANN-accredited registrars of internet domain names. WIPO is accredited by ICANN as a domain name dispute resolution service provider.[198] Since then WIPO Centre has been providing ODR services for resolving domain name disputes and has administered over 30,000 proceedings, of which over 15,000 have been under the WIPO-UDRP adopted by ICANN.[199]

In December 2008 WIPO submitted a proposal, 'eUDRP Initiative',[200] to ICANN. The eUDRP Initiative proposed to remove the requirement to submit and distribute paper copies of pleadings relating to the UDRP process, primarily through the use of email in order to eliminate the use of vast quantities of paper and improve the timeliness of UDRP proceedings without prejudicing either complainants or respondents.[201]

Scholars identify the reasons for the success of the WIPO-UDRP domain name dispute resolution system, such as credibility, transparency, self-enforcement, accountability, etc.[202] Firstly, WIPO and ICANN are both pubic organisations with authorities. WIPO's participation in dealing with domain main disputes particularly adds **credibility** to the process due to its professional expertise and resources. Secondly, every dot.com registrant is **compulsorily** governed by the WIPO-UDRP without conflict of rules and procedures when disputes occur. Thirdly, domain name case decisions are available online immediately in full text,[203] which increases **transparency** of the procedure and imposes a degree of public **accountability**, which protects the rights of lawful domain name holders. Fourthly, the case is usually closed two months after filing and an administrative panel decision is implemented by the registrar 10 days after the decision is rendered.[204] No foreign authorities can block the outcome, which promotes the **enforceability** of settlement. Lastly, but most importantly, WIPO provides an **efficient** domain name dispute resolutions service, as all complaints and responses can be completed and submitted directly online.[205] The supplementary rule of the eUDRP Initiative reflects on the efforts of WIPO on promoting efficiency and improving **quality** in domain name online dispute resolutions.

CIETAC and HKIAC

China and Hong Kong enacted the 'One Country, Two Systems' policy, which means that the laws in Hong Kong will be different from those in China. The business link between China and Hong Kong is very close. Lots of companies have their headquarters in China but branches in Hong Kong, or vice versa. If a company registers a .com or .net domain name and has offices in both China and Hong Kong it can file a case when its rights in domain names are infringed.

To bridge the two systems the Asian Domain Name Dispute Resolution Centre (ADNDRC) was set up as a joint undertaking of the China International Economic and Trade Arbitration Commission (CIETAC) and the Hong Kong International Arbitration Centre (HKIAC) to deal with

gTLDs (.com/.org) domain name disputes.[206] There are two offices – Beijing and Hong Kong – in the Asian Domain Names Dispute Resolution Centre. Both offices comply with the same policy – WIPO UDRP for gTLDs disputes. Complainants can choose one of them to file a case.

At the same time both CIETAC in Beijing and HKIAC in Hong Kong are also appointed by the China Internet Network Information Center (CNNIC) providing dispute resolution services with regard to .CN domain names, known as 'CIETAC Domain Name Dispute Resolution Centre'[207] and 'HKIAC .cn Domain Name Resolution Centre'.[208] The .CN domain name disputes are carried out under the CNNIC Domain Name Dispute Resolution Policy (CNDRP)[209] in both the China and Hong Kong centres, while HKIAC uses its own policy for .HK disputes.

With these two ODR service providers (CIETAC and HKIAC) the complainant should submit the Complaint Form and submit it in electronic form by email.[210] Generally a decision should be made on the basis of the statements and documents submitted by the parties. A panel has 14 days to render a decision.[211] The panel's decision will be submitted both in electronic and paper form signed by all the panellists. The decisions will be published on the websites of the service providers, except in special circumstances.[212]

For example, the case *Avon Products, INC v Ni Ping*[213] was filed with ADNDRC Beijing Office on 27 April 2007. The complainant is one of the world's most well known direct sellers of cosmetic products. The claimant claims that since 1886 it has built up distribution networks covering 145 countries, 8 million customers and 4.8 million independent sales representatives. The claimant has expended extensive amounts of fiscal and temporal capital in preserving the value of its AVON and 'Ya Fang' trademarks in Roman and Chinese characters, including registration of these trademarks throughout the world, including mainland China, Hong Kong, Taiwan and Singapore. It entered into the PRC market in 1990 and now has 77 branches in China and over 6,000 specialty shops; and sales between 2000 and 2004 of products marked with 'Ya Fang' in Chinese characters (or derivative marks) totalled over US$681 million, thereby providing substantial evidence of a global association of the complainant's 'Ya Fang' marks with its cosmetic products. The claimant asserted that the respondent's use of domain name 'yafang.net', which was registered on 12 August 2003 in Beijing, would confuse existing and future customers and constitute use and registration in bad faith. When visitors type in www.yafang.net, it will directly connect to www.x-y-f.com. The respondent Ni Ping also registered 'avon.cn', 'yafang.cn' and 'niping.cn' on 17 March 2003, and sold cosmetic products online. Ni Ping transferred the link of 'yafang.net' to 'avon.cn', 'yafang.cn' and 'niping.cn' after the complaint was filed. The Panel ordered that the domain name 'yafang.net' be transferred to the complainant, pursuant to Article 4(a) of the UDRP.

In the author's opinion the characteristics or advantages of CIETAC and HKIAC ODR services for domain name disputes are very similar to the

WIPO domain dispute resolution service in terms of efficiency, accountability, transparency and self-enforceability. The CIETAC and HKIAC centres provide valuable experiments and cornerstones for developing a Chinese ODR system for disputes arising from e-commerce transactions. The launch of the Asian Domain Name Dispute Resolution Centre successfully combined the two systems in China and Hong Kong – in one country. It serves as a joint venture providing domain name online dispute resolutions, which generate consistency, harmony and certainty.

Summary: lessons to be learned

The ICANN and WIPO-UDRP, eBay and SquareTrade, AAA and Cybersettle, CIETAC and HKIAC – the four successful examples of international ODR practices – provide a tremendous amount of valuable experience:

Firstly, they provide advanced technology support and make a very attractive offer for easily accessible, quick, effective, and low-cost dispute resolution. For example, eBay users only need to pay US$15 for the online mediation service provided by SquareTrade, and if they choose automated online negotiation to resolve their trade disputes, it will even be free.[214] The mediation process on SquareTrade for eBay users generally takes only 10 days.[215]

Secondly, they have succeeded in integrating their offer to the primary markets.[216] The four ODR services mainly target resolving e-commerce related disputes; for example, the SquareTrade dispute resolution service provider deals with eBay users' online trading disputes. WIPO-UDRP or CIETAC and HKIAC deal with ICANN domain names users' disputes.

Thirdly, the integration is brought about by co-operation agreements with the primary market makers. For example, SquareTrade is appointed by eBay (a primary market maker) for resolving eBay users' trading disputes. AAA and Cybersettle create a strategic alliance. WIPO-UDRP is accredited by ICANN as the domain name dispute service provider, while CIETAC and HKIAC are accredited by ADNDRC.

Fourthly, the ODR service is promoted by creating socio-legal bonds for potential dispute parties to commit to the process.[217] That is, the ICANN UDRP administrative procedure is mandatory to domain name holders, whilst the SquareTrade mediation process is mandatory to eBay-sellers.

Fifthly, the self-enforcement or self-execution mechanisms to enforce dispute settlements are a credential that makes ODR services successful. For example, ICANN and WIPO have self-enforcement mechanisms. The ICANN-accredited registrars have the right to transfer or cancel a domain name directly when the decision of settlement is made.[218]

Sixthly, ODR service has the expertise to resolve certain internet disputes, such as cross-border small claim disputes and domain names disputes. Take the feature of domain name disputes equipped with ODR service as an example. The growth in the use of domain names appears to have increased the number of bad faith registrations and further raised concerns that trade mark owners' rights are increasingly infringed or diluted by the use of trade marks in domain names.[219] That is, domain names have come into conflict with trade marks. The main reason for such conflict can be attributed to the lack of connection between the system of registering trade marks and the registration of domain names. The former is a system granting territorial rights enforceable only within the designated territory; the latter is a system of granting rights that can be enforced globally.[220] Because trade mark law is territorial, a mark may be protected only in the geographic location where it distinguishes its goods or services. Thus, trade mark law can tolerate identical or similar marks in different territories even within the same classes of goods and services. Domain names, by contrast, are both unique and global in nature.[221] Only one entity in the world can own the right to use a specific domain name that can be accessed globally.[222] According to the specific features of a domain name, in particular, without territory but with a registrar, ODR will be one of the most suitable methods to resolve domain names disputes.

10.3.3 The future of ODR: international standardisation

ODR not only provides speedy and cost-effective techniques in resolving cross-border disputes, but also boosts trust and confidence in electronic commercial transactions in the e-marketplace, because it diminishes the risk that e-commerce users are left with no redress if contracts are not performed.[223] A continuing challenge and demand for resolving cross-border commercial disputes resulting from globalisation calls for the improvement of ODR services. International standardisation of ODR services should be deemed as a measure to enhance the quality of its services. International standardisation can possibly be reached through the promulgation of regulations, codes of conduct, guidelines, frameworks, model laws or even conventions by international legislative organisations.

A number of provisions should be considered and included in such an international ODR service legislative instrument:

1 ODR service providers should encourage, by any means which they consider appropriate, the development of the ODR system generating a balanced function of convenience, trust and expertise.

   Convenience, trust and expertise are generally not independent of each other. In other words, if the level of one factor is changed the level of some other factor may be affected. Raising one factor a lot may lower another factor a little, often a beneficial trade-off. Or, raising one factor a

lot may, at the same time, also raise the level of some other factor, almost certainly a desirable outcome.[224] Therefore, the balance of the three elements can contribute to the building of a more user-friendly and efficient ODR system.

2 ODR service providers should ensure that the content of a mediation agreement or arbitral award is enforceable, or may be made enforceable by a court or other competent authority in a judgment.

The validity of the mediation settlement and arbitral award as to form is one of the obstacles of ODR services. The ODR service provider should clearly provide mediation rules or procedures about the validity and enforcement of a mediation settlement. A mediation settlement may be valid when it is signed by both parties according to the mediation agreement. Or if parties pre-agree an open basis the mediation settlement may be agreed upon during the mediation process or after the mediation, either expressly or impliedly. For example, in the UK case *Brown v Rice*,[225] both parties agreed to mediate and entered into a mediation agreement, which provided that any settlement reached in the course of the mediation would not be binding until it was reduced to writing and signed by, or on behalf of, the parties. The judge held that no binding agreement was reached because it was never reduced to writing and signed by, or on behalf of, each of the parties, as required by the mediation agreement, although Brown argued that on the morning following the mediation he agreed to the settlement made the previous evening.

The EC Directive on Mediation in 2008 is also aware of the importance of this issue and it aims to ensure the enforceability of agreements resulting from mediation.[226] For example, the EC Directive on Mediation enables parties to request a written agreement concluded following mediation. It is specified that the content of the agreement is similar to a court judgment, which shall be made enforceable. Such a mediation agreement can be achieved by way of 'a court or other competent authority in a judgment or decision or in an authentic instrument'.[227]

3 ODR service providers shall ensure that, unless the parties agree otherwise, the disputants' personal information, the materials of evidence and the decision of settlement will be kept confidential.

Confidentiality is one of the challenging issues of ODR services, as it conflicts with accountability which is one of the fundamental principles of ODR service. Confidentiality seems to be upheld in most of the ODR self-regulation rules as it is linked with the protection of trade secrets and individual privacy. One of the reasons that parties choose out-of-court dispute resolutions is that they don't feel comfortable being exposed to the public. Moreover, when parties choose out-of-court dispute resolutions, particularly in an electronic platform (so called 'ODR'), sometimes it may also mean that they don't even feel comfortable with resolving the dispute face-to-face. The EC Directive on Mediation supports the enhancement of the confidentiality of mediation[228] by preventing

mediators or those involved in the mediation process from giving information or evidence in civil and commercial judicial proceedings or arbitration.[229] However, in order to boost confidence and increase usage of ODR services, ODR providers should still be allowed to disclose certain mediation settlements or arbitral awards by pre-agreement with users.

SquareTrade provides a good pioneer experience in balancing the rights of confidentiality and accountability. As discussed, accountability hinges on transparency and structure, while mediation's strength is drawn, to a large extent, from its confidentiality and flexibility.[230] An essential component in SquareTrade's accountability system is its substantial database on resolution efforts. SquareTrade has managed to gather extensive information internally without completely foregoing confidentiality externally. SquareTrade collects a vast amount of information on the services it provides, which will remain accessible to SquareTrade, the mediator and the parties for up to one year. SquareTrade also collects other data information through the seal program and users' registration. SquareTrade also records 'Resolution Behaviour Information' at the end of ODR service, which contains information on whether a party participated in the process to completion, whether an agreement was reached, whether the party accepted or rejected a mediator's recommendation, and, with respect to a respondent, whether the person had been involved in multiple cases of this type.[231] Such data will be kept confidential, but the outcome of statistics can be used in the market promotion analysis of ODR service.

4 ODR service providers shall ensure that, by any means which they consider appropriate, the code of conduct of ODR services, including administrative duties and procedures, will be made available to the general public.

It should include, as recommended by the ABA Task Force on E-commerce and ADR Recommended Best Practices for Online Dispute Resolution Service Providers: (i) publishing statistical reports; (ii) employing identifiable and accessible data formats; (iii) presenting printable and downloadable information; (iv) publishing decisions with whatever safeguards necessary to prevent party identification; (v) describing the types of services provided; (vi) affirming due process guarantees; (vii) disclosing minimum technology requirements to utilise the provider's technology; (viii) disclosing all fees and expenses to use ODR services; (ix) disclosing qualifications and responsibilities of neutrals; (x) disclosing jurisdiction, choice of law and enforcement clauses; for example, ODR providers should disclose the jurisdiction where complaints against the ODR provider can be brought, and any relevant jurisdictional limitations.[232]

5 ODR service providers shall encourage, by any means appropriate, the use of Trust Mark Schemes in online trading or service and voluntarily provide out-of-court dispute resolutions to those disputes. Such schemes

> are used to establish trust in electronic commerce, ensure the global order of online electronic commercial transactions and protect the fundamental human right of privacy.
>
> ODR service providers can also boost the confidence of commercial website users by assisting the operation of trust programs or directly offering seal programs. For example, the SquareTrade seal program is a distinctive eBay service. Under this system, Square Trade verifies the identity and address of eBay sellers, who, in return, commit to a specified set of selling standards and pay a low fee to SquareTrade. The seal is an icon that is displayed by the seller's ID on eBay but remains under the complete control of SquareTrade. SquareTrade can follow trends on buyer activities and habits since these patterns are recorded when buyers click on the seal. It can also remove the seal icon at any time should a seller no longer meet the requirements.[233]

In conclusion, from the examination of the four successful examples of eBay with SquareTrade, AAA with Cybersettle, ICANN with WIPO–UDRP, as well as CIETAC and HKIAC it can be suggested that the corporation agreement of ODR service providers and primary market makers, the expertise of technological and legal issues in internet-related disputes, the self-enforcement mechanism of resolution outcomes, are key factors for their success, as well as the other measures that bolster users' trust and confidence in doing business online.

In the author's view international ODR guidelines are needed to harmonise the standard of ODR services in the global market. Such international instruments should clarify at least five main areas as evaluated earlier – appropriation of ODR technology, protection of confidentiality, conditions of enforceability, requirements of ODR administration and implementation of trust mark schemes.

Meanwhile, national legislative organisations should amend or update the offline ADR rules by recognising electronic means of communication in resolving disputes and incorporating concepts of online dispute resolution.

Part V

The future

11 Conclusions and recommendations

11.1 Future legislative trends in the EU, US and China

The advance of information technology creates new patterns of commercial enterprises and changes the life of individuals. It changes the essence of traditional paper-based and face-to-face international trade and domestic business. Buying and selling online has become a common practice without regard to physical meetings and geographical boundaries. The ever-increasing usage of the internet has dramatically driven an explosion of electronic commerce. Legal challenges are emerging.

Broadly, the law of electronic commercial transactions should promote free and fair trade between nations and within nations. In a narrow scope, the law of electronic commercial transactions should regulate the conduct of businesses and individuals online. The law of electronic commercial transactions is within the regime of traditional commercial law and international trade law, covering wide-ranging legal issues. However, it also challenges the legal recognition of the validity of electronic contracts because traditional laws were promulgated before the widespread use of electronic commerce and without consideration of the usage of electronic means.

International, regional and national legislative organisations have been making efforts to produce particularised legal instruments to facilitate the development of electronic commerce. There are different approaches adopted in those organisations equipped for different cultural and economic situations. The EU intends to establish comprehensive rules in directives and regulations for Member States. The US prefers to adopt a market-oriented approach encouraging self-regulation. China chooses to adopt subject-specific international instruments, i.e. conventions or model laws to keep up with the international standard. During this ongoing legislative process in the laws of electronic commercial transactions, nations have faced some similar problems:

Firstly, it is argued that electronic commerce does not add new insights into the operation of traditional laws, such as contract law; instead, it adds a different layer of communication by electronic means, and thus a new body of laws governing issues in electronic commercial transactions would not

need to be established.[1] Although it would avoid causing confusion and complicating the legal system unnecessarily, it is debatable whether the traditional laws are sufficient and efficient enough to deal with newly emerging e-disputes.

Secondly, the majority of transnational electronic transactions involve people that will never physically meet. How to create trust and establish confidence in online interaction and transactions is challenging for international, regional and national law makers. Promoting trust and confidence in electronic commerce is one of the prioritised aims in laws of electronic commercial transactions.

Harmonisation or convergence of national laws, whether by international conventions or model laws, conscious or unconscious judicial parallelism or uniform rules for specified types of contract will remove the obstacles of transnational commercial transactions. In the author's opinion it is understandable that it would cause confusion if there were two sets of international and national trade laws, one for offline and the other for online. It is normal to doubt the practicality of such an approach. But fear of facilitating different sets of laws should not become an obstacle to modernising existing laws to adapt to the future development of various technologies in electronic commercial transactions. From the research in this book there is strong evidence that electronic commercial transactions do have their unique characteristics. The entire concept of electronic transactions is the same as the traditional ones, but the actual conduct of electronic transactions is fundamentally different.

It is certain that electronic transactions can be deemed to be a means of communication from a technological point of view. However, from a legal perspective, there are two dominant factors that could distinguish the legal consequences of electronic transactions from traditional ones – the determination of 'time and place of dispatch and receipt of an electronic communication',[2] and 'the place of business'[3] in cyberspace. When involving digitised goods with delivery online, these two factors, as explained in the book, would lead to different outcomes in relation to ascertaining the rules of electronic offer and acceptance, jurisdiction and applicable law. Traditional contract law and private international law will not be sufficient to govern these issues.

It is notable that before drafting completely new electronic commerce laws, careful consideration should be given to existing laws. If nations decide not to produce new laws for electronic commerce it is recommended that those nations adopt the international instruments in electronic commerce in order to promote an international trade relationship. An explanatory note to the existing laws should be also produced to explain and complement the legal issues of electronic commerce. If nations decide to have particularised legislation, they can either insert new provisions of electronic commerce into existing laws as well as modernise the existing provisions, or create new sets of laws in electronic commercial transactions.

Some IT specific legal issues concerning electronic signatures and authentication, as well as the conduct of online dispute resolution, should be regulated in a separate set of laws because, although requirements of signature as well as rules of litigation, arbitration, mediation and negotiation can remain the same as the offline legislation, using electronic means creates new concepts, raises new issues and challenges the validity of evidence in these legal areas.

Most of the nations have made efforts to remove legal barriers to electronic commerce. International legislative organisations push forward the process of the harmonisation of international electronic commerce by proposing general principles to create confidence for doing business online. However, some legal obstacles to electronic commercial transactions remain unresolved as there is a lack of substantive rules.

11.2 Solutions to obstacles in the law of electronic commercial transactions

The book proposes solutions to the eight main legal obstacles to electronic commercial transactions as highlighted in Part I.

The first solution concerns the determination of electronic offer and acceptance in electronic contracts. After examining the characteristics of electronic communications, including email contracting and clickwrap agreements, it is concluded that a contract formed by electronic means is similar to a contract made by telephone or facsimile as they are all instantaneous. Although dispatching an email is like dropping a letter in a red post box, email communication is much quicker than traditional post. Electronic mail overcomes the disadvantages of the postal mail as it is possible to determine the time of dispatch and receipt of electronic communications, providing evidential certainty as to the receipt of an offer and acceptance. Therefore the postal rule loses its purpose in electronic communications. Where an offer and acceptance are to be communicated by electronic means a contract should be concluded upon receipt of the acceptance by the offeror. The author's proposal is that the acceptance rule should prevail over the postal rule in electronic offer and acceptance. Hence, the acceptance should be effective when it is received.

The second solution refers to the availability of contract terms, errors in electronic communications, and battle of forms. In relation to the availability of contract terms, most current e-commerce legislation does not require such a duty. In the author's view, it is necessary for model laws, directives or conventions to impose a duty of making contract terms available or reproducible online, because it is crucial to have evidence when disputes arise. With regard to errors in electronic communications, technologies enabling the amendment in error inputs and the withdrawal of error communications must be available on the website, because in instantaneous and automated communications, negligence can appear easily and unintentionally. For example, pressing the wrong button on the internet can create serious legal

consequences. The time restriction of notification of error in electronic communications should also be defined. Referring to battle of forms, the combination of the ruling in the UCC, CISG, PICC, PECL and CLC can apply to online battle of forms, that is, electronic acceptance which contains additions, limitations or other modifications, is a rejection of the offer and constitutes a counter-offer. However, if the additional or different terms in the general conditions of the acceptance do not materially alter the offer, they should form part of the contract to the extent that they are common in substance, or otherwise parties agree.

The third solution focuses on the removal of barriers to the recognition of electronic signatures and authentication, in particular, recognition of foreign certificates and electronic signatures. An electronic signature is essential because it identifies the contracting parties, secures the electronic transactions and indicates recognition and approval of the contents of a document. In all the existing electronic signatures laws, electronic signatures have been recognised as equivalent to handwritten signatures. Certificate Authorities (CAs), trusted third parties, can be licensed or unlicensed, public or private. The industry of CAs has not developed as expected since the 1990s because private sector entities are reluctant to establish CAs due to the uncertainty of their legal liability. There are no substantive rules governing the standard of an electronic signature and the recognition of foreign certificates of authentication. In the author's view, the establishment of a model law regulating the conduct of international certificate authorities is necessary because electronic commercial transactions are often transnational and there is a high risk of dealing with fraudulent certificates from a third country. Furthermore, parties using foreign certificates will have no certainty of legal protection because national laws are different.

The fourth solution tackles the sufficiency of technical measures and legal protocols of data privacy protection. Data privacy security is vital in creating users' trust and confidence in online interaction and transactions. On the other hand, the free flow of data information between different nations is necessary to stimulate international business transactions and globalisation. In the information society, legislation of data privacy protection should be equipped to keep the balance between the free flow of data information and the fundamental human right of privacy. Self-regulation in data privacy protection has also been encouraged by international legislative instruments; however, there should be procedures in laws examining whether companies strictly comply with their privacy policies. Private trusted third parties services, such as TRUSTe program, can also provide supervision and enhance enforceability to data privacy protection in companies.

The fifth solution focuses on the issue of ascertaining jurisdiction in electronic contracts. There are different rules of jurisdiction in the EU, US and China. The EU applies general and special jurisdiction according to the Brussels I Regulation, whilst the US Courts, following the *International Shoe* case, focus on whether a defendant's activities constitute 'minimum contacts'

with a forum state, as well as applying the sliding scale from the *Zippo* case which distinguishes between three broad categories of websites based on their interactive and commercial characteristics. Chinese law is different from that of the EU and the US as it does not address provisions of general and special jurisdiction separately. However, Chinese law, just like in the EU and the US, favours two factors, domicile and the place of performance, to determine jurisdiction. This book concludes that for disputes involving contracts of tangible or digitised goods with physical delivery, rules of internet jurisdiction are the same as the rules of offline jurisdiction, as the place of performance has a physical location in both. However, for disputes involving contracts of digitised goods with delivery online, the rule concerning the place of performance online must be specifically examined. In the author's view, in this case, the place of performance should be the recipient's place of business indicated by the party. If the party fails to indicate the place of business or has more than one place of business, the place of business should be the one with the closest relationship to the relevant contract or where the principal place of business is situated.

The sixth solution refers to determining the applicable law in electronic contracts. The EU, US and China distinguish the applicable law in cases of choice and in absence of choice by parties. As a general rule parties are free to choose the governing law. Otherwise the contract will be governed by the law of the country with which the contract is most closely connected or has the most significant relationship to the transaction in cases of absence of express choice. Just as in the determination of internet jurisdiction, tangible or digitised goods transacted online with physical delivery do follow the same rules for the determination of the applicable law as in the offline world. The difference arises with contracts involving digitised goods with delivery online. According to the findings in the book, in this case, the seller's place of business is the most enduring connecting factor, which has an economic impact on its area. Thus, the law of the seller's place of business should be the law governing B2B electronic contracts in the absence of a choice of law clause.

The seventh solution aims to clarify the mechanism of online dispute resolution (ODR) referring to electronic contracting disputes. ODR is a new solution to build trust in electronic commercial transactions. Four successful examples, WIPO with UDRP, eBay with SquareTrade, AAA with Cybersettle and CIETAC with HKIAC have been examined in this book, proving that the linking of ODR service providers and primary market makers, as well as the self-enforcement mechanism of resolution outcomes, are key credentials to their success. The conduct of ODR should include six core principles: accountability, confidentiality, accessibility, credibility, security and enforceability. Enforceability is essential, since its success will encourage electronic traders or businesses to use ODR to resolve their disputes. The outcome of online mediation and negotiation should be easily converted into settlement agreements, whilst the decisions of online arbitration should constitute arbitral awards.

Otherwise, the ODR service providers should have self-enforcement or self-execution mechanisms to enforce contractual dispute settlements.

The eighth solution relates to the lack of trust in online business transactions. Building trust and confidence in electronic commerce not only requires the availability and knowledge of advanced information technology but also legal protection. The technical infrastructure and legal framework of building e-trust and e-confidence, as the theme of the book, have been discussed, analysed and evaluated throughout the subject matter of the validity of electronic contract, the recognition of domestic and foreign certificates and electronic signatures, the measures of data privacy protection, the determination of internet jurisdiction and choice of law, as well as the efficiency and suitability of online dispute resolution.

Overall, during the pre-internet era companies traded with foreign companies even though their legal systems were different. The absence of unified laws did not prevent them from conducting effective cross-border business. Therefore, unifying electronic commerce laws should not be regarded as a significant legal impediment. Modernisation, harmonisation and facilitation of the law of electronic commercial transactions at the international level should be continually employed in building e-trust and e-confidence.

Appendix 1: United Nations Convention on the Use of Electronic Communications in International Contracts 2005

The States Parties to this Convention,
Reaffirming their belief that international trade on the basis of equality and mutual benefit is an important element in promoting friendly relations among States,

Noting that the increased use of electronic communications improves the efficiency of commercial activities, enhances trade connections and allows new access opportunities for previously remote parties and markets, thus playing a fundamental role in promoting trade and economic development, both domestically and internationally,

Considering that problems created by uncertainty as to the legal value of the use of electronic communications in international contracts constitute an obstacle to international trade,

Convinced that the adoption of uniform rules to remove obstacles to the use of electronic communications in international contracts, including obstacles that might result from the operation of existing international trade law instruments, would enhance legal certainty and commercial predictability for international contracts and help States gain access to modern trade routes,

Being of the opinion that uniform rules should respect the freedom of parties to choose appropriate media and technologies, taking account of the principles of technological neutrality and functional equivalence, to the extent that the means chosen by the parties comply with the purpose of the relevant rules of law,

Desiring to provide a common solution to remove legal obstacles to the use of electronic communications in a manner acceptable to States with different legal, social and economic systems,

Have agreed as follows:

Chapter I
Sphere of application
Article 1
Scope of application

1. This Convention applies to the use of electronic communications in connection with the formation or performance of a contract between parties whose places of business are in different States.
2. The fact that the parties have their places of business in different States is to be disregarded whenever this fact does not appear either from the contract or from any dealings between the parties or from information disclosed by the parties at any time before or at the conclusion of the contract.
3. Neither the nationality of the parties nor the civil or commercial character of the parties or of the contract is to be taken into consideration in determining the application of this Convention.

Article 2
Exclusions

1. This Convention does not apply to electronic communications relating to any of the following:
(*a*) Contracts concluded for personal, family or household purposes;
(*b*) (i) Transactions on a regulated exchange; (ii) foreign exchange transactions; (iii) inter-bank payment systems, inter-bank payment agreements or clearance and settlement systems relating to securities or other financial assets or instruments; (iv) the transfer of security rights in sale, loan or holding of or agreement to repurchase securities or other financial assets or instruments held with an intermediary.
2. This Convention does not apply to bills of exchange, promissory notes, consignment notes, bills of lading, warehouse receipts or any transferable document or instrument that entitles the bearer or beneficiary to claim the delivery of goods or the payment of a sum of money.

Article 3
Party autonomy

The parties may exclude the application of this Convention or derogate from or vary the effect of any of its provisions.

Chapter II
General provisions
Article 4
Definitions

For the purposes of this Convention:
(*a*) 'Communication' means any statement, declaration, demand, notice or request, including an offer and the acceptance of an offer, that the parties are required to make or choose to make in connection with the formation or performance of a contract;

(*b*) 'Electronic communication' means any communication that the parties make by means of data messages;
(*c*) 'Data message' means information generated, sent, received or stored by electronic, magnetic, optical or similar means, including, but not limited to, electronic data interchange, electronic mail, telegram, telex or telecopy;
(*d*) 'Originator' of an electronic communication means a party by whom, or on whose behalf, the electronic communication has been sent or generated prior to storage, if any, but it does not include a party acting as an intermediary with respect to that electronic communication;
(*e*) 'Addressee' of an electronic communication means a party who is intended by the originator to receive the electronic communication, but does not include a party acting as an intermediary with respect to that electronic communication;
(*f*) 'Information system' means a system for generating, sending, receiving, storing or otherwise processing data messages;
(*g*) 'Automated message system' means a computer program or an electronic or other automated means used to initiate an action or respond to data messages or performances in whole or in part, without review or intervention by a natural person each time an action is initiated or a response is generated by the system;
(*h*) 'Place of business' means any place where a party maintains a nontransitory establishment to pursue an economic activity other than the temporary provision of goods or services out of a specific location.

Article 5
Interpretation
1. In the interpretation of this Convention, regard is to be had to its international character and to the need to promote uniformity in its application and the observance of good faith in international trade.
2. Questions concerning matters governed by this Convention which are not expressly settled in it are to be settled in conformity with the general principles on which it is based or, in the absence of such principles, in conformity with the law applicable by virtue of the rules of private international law.

Article 6
Location of the parties
1. For the purposes of this Convention, a party's place of business is presumed to be the location indicated by that party, unless another party demonstrates that the party making the indication does not have a place of business at that location.
2. If a party has not indicated a place of business and has more than one place of business, then the place of business for the purposes of this Convention is that which has the closest relationship to the relevant contract, having regard to the circumstances known to or contemplated by the parties at any time before or at the conclusion of the contract.

3. If a natural person does not have a place of business, reference is to be made to the person's habitual residence.
4. A location is not a place of business merely because that is: (*a*) where equipment and technology supporting an information system used by a party in connection with the formation of a contract are located; or (*b*) where the information system may be accessed by other parties.
5. The sole fact that a party makes use of a domain name or electronic mail address connected to a specific country does not create a presumption that its place of business is located in that country.

Article 7
Information requirements
Nothing in this Convention affects the application of any rule of law that may require the parties to disclose their identities, places of business or other information, or relieves a party from the legal consequences of making inaccurate, incomplete or false statements in that regard.

Chapter III
Use of electronic communications in international contracts
Article 8
Legal recognition of electronic communications
1. A communication or a contract shall not be denied validity or enforceability on the sole ground that it is in the form of an electronic communication.
2. Nothing in this Convention requires a party to use or accept electronic communications, but a party's agreement to do so may be inferred from the party's conduct.

Article 9
Form requirements
1. Nothing in this Convention requires a communication or a contract to be made or evidenced in any particular form.
2. Where the law requires that a communication or a contract should be in writing, or provides consequences for the absence of a writing, that requirement is met by an electronic communication if the information contained therein is accessible so as to be usable for subsequent reference.
3. 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.

4. Where the law requires that a communication or a contract should be made available or retained in its original form, or provides consequences for the absence of an original, that requirement is met in relation to an electronic communication if:

(*a*) There exists a reliable assurance as to the integrity of the information it contains from the time when it was first generated in its final form, as an electronic communication or otherwise; and

(*b*) Where it is required that the information it contains be made available, that information is capable of being displayed to the person to whom it is to be made available.

5. For the purposes of paragraph 4 (*a*):

(*a*) The criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change that arises in the normal course of communication, storage and display; and

(*b*) The standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

Article 10

Time and place of dispatch and receipt of electronic communications

1. The time of dispatch of an electronic communication is the time when it leaves an information system under the control of the originator or of the party who sent it on behalf of the originator or, if the electronic communication has not left an information system under the control of the originator or of the party who sent it on behalf of the originator, the time when the electronic communication is received.

2. The time of receipt of an electronic communication is the time when it becomes capable of being retrieved by the addressee at an electronic address designated by the addressee. The time of receipt of an electronic communication at another electronic address of the addressee is the time when it becomes capable of being retrieved by the addressee at that address and the addressee becomes aware that the electronic communication has been sent to that address. An electronic communication is presumed to be capable of being retrieved by the addressee when it reaches the addressee's electronic address.

3. An electronic communication is deemed to be dispatched at the place where the originator has its place of business and is deemed to be received at the place where the addressee has its place of business, as determined in accordance with article 6.

4. Paragraph 2 of this article applies notwithstanding that the place where the information system supporting an electronic address is located may be different from the place where the electronic communication is deemed to be received under paragraph 3 of this article.

Article 11
Invitations to make offers
A proposal to conclude a contract made through one or more electronic communications which is not addressed to one or more specific parties, but is generally accessible to parties making use of information systems, including proposals that make use of interactive applications for the placement of orders through such information systems, is to be considered as an invitation to make offers, unless it clearly indicates the intention of the party making the proposal to be bound in case of acceptance.

Article 12
Use of automated message systems for contract formation
A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, shall not be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems or the resulting contract.

Article 13
Availability of contract terms
Nothing in this Convention affects the application of any rule of law that may require a party that negotiates some or all of the terms of a contract through the exchange of electronic communications to make available to the other party those electronic communications which contain the contractual terms in a particular manner, or relieves a party from the legal consequences of its failure to do so.

Article 14
Error in electronic communications
1. Where a natural person makes an input error in an electronic communication exchanged with the automated message system of another party and the automated message system does not provide the person with an opportunity to correct the error, that person, or the party on whose behalf that person was acting, has the right to withdraw the portion of the electronic communication in which the input error was made if:
(*a*) The person, or the party on whose behalf that person was acting, notifies the other party of the error as soon as possible after having learned of the error and indicates that he or she made an error in the electronic communication; and
(*b*) The person, or the party on whose behalf that person was acting, has not used or received any material benefit or value from the goods or services, if any, received from the other party.
2. Nothing in this article affects the application of any rule of law that may govern the consequences of any error other than as provided for in paragraph 1.

Chapter IV
Final provisions
Article 15
Depositary
The Secretary-General of the United Nations is hereby designated as the depositary for this Convention.

Article 16
Signature, ratification, acceptance or approval
1. This Convention is open for signature by all States at United Nations Headquarters in New York from 16 January 2006 to 16 January 2008.
2. This Convention is subject to ratification, acceptance or approval by the signatory States.
3. This Convention is open for accession by all States that are not signatory States as from the date it is open for signature.
4. Instruments of ratification, acceptance, approval and accession are to be deposited with the Secretary-General of the United Nations.

Article 17
Participation by regional economic integration organizations
1. A regional economic integration organization that is constituted by sovereign States and has competence over certain matters governed by this Convention may similarly sign, ratify, accept, approve or accede to this Convention.
The regional economic integration organization shall in that case have the rights and obligations of a Contracting State, to the extent that that organization has competence over matters governed by this Convention. Where the number of Contracting States is relevant in this Convention, the regional economic integration organization shall not count as a Contracting State in addition to its member States that are Contracting States.
2. The regional economic integration organization shall, at the time of signature, ratification, acceptance, approval or accession, make a declaration to the depositary specifying the matters governed by this Convention in respect of which competence has been transferred to that organization by its member States. The regional economic integration organization shall promptly notify the depositary of any changes to the distribution of competence, including new transfers of competence, specified in the declaration under this paragraph.
3. Any reference to a 'Contracting State' or 'Contracting States' in this Convention applies equally to a regional economic integration organization where the context so requires.
4. This Convention shall not prevail over any conflicting rules of any regional economic integration organization as applicable to parties whose respective places of business are located in States members of any such organization, as set out by declaration made in accordance with article 21.

Article 18
Effect in domestic territorial units
1. If a Contracting State has two or more territorial units in which different systems of law are applicable in relation to the matters dealt with in this Convention, it may, at the time of signature, ratification, acceptance, approval or accession, declare that this Convention is to extend to all its territorial units or only to one or more of them, and may amend its declaration by submitting another declaration at any time.
2. These declarations are to be notified to the depositary and are to state expressly the territorial units to which the Convention extends.
3. If, by virtue of a declaration under this article, this Convention extends to one or more but not all of the territorial units of a Contracting State, and if the place of business of a party is located in that State, this place of business, for the purposes of this Convention, is considered not to be in a Contracting State, unless it is in a territorial unit to which the Convention extends.
4. If a Contracting State makes no declaration under paragraph 1 of this article, the Convention is to extend to all territorial units of that State.

Article 19
Declarations on the scope of application
1. Any Contracting State may declare, in accordance with article 21, that it will apply this Convention only:
(*a*) When the States referred to in article 1, paragraph 1, are Contracting States to this Convention; or
(*b*) When the parties have agreed that it applies.
2. Any Contracting State may exclude from the scope of application of this Convention the matters it specifies in a declaration made in accordance with article 21.

Article 20
Communications exchanged under other international conventions
1. The provisions of this Convention apply to the use of electronic communications in connection with the formation or performance of a contract to which any of the following international conventions, to which a Contracting State to this Convention is or may become a Contracting State, apply:

Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York, 10 June 1958);

Convention on the Limitation Period in the International Sale of Goods (New York, 14 June 1974) and Protocol thereto (Vienna, 11 April 1980);

United Nations Convention on Contracts for the International Sale of Goods (Vienna, 11 April 1980);

United Nations Convention on the Liability of Operators of Transport Terminals in International Trade (Vienna, 19 April 1991);

United Nations Convention on Independent Guarantees and Stand-by Letters of Credit (New York, 11 December 1995);

United Nations Convention on the Assignment of Receivables in International Trade (New York, 12 December 2001).

2. The provisions of this Convention apply further to electronic communications in connection with the formation or performance of a contract to which another international convention, treaty or agreement not specifically referred to in paragraph 1 of this article, and to which a Contracting State to this Convention is or may become a Contracting State, applies, unless the State has declared, in accordance with article 21, that it will not be bound by this paragraph.

3. A State that makes a declaration pursuant to paragraph 2 of this article may also declare that it will nevertheless apply the provisions of this Convention to the use of electronic communications in connection with the formation or performance of any contract to which a specified international convention, treaty or agreement applies to which the State is or may become a Contracting State.

4. Any State may declare that it will not apply the provisions of this Convention to the use of electronic communications in connection with the formation or performance of a contract to which any international convention, treaty or agreement specified in that State's declaration, to which the State is or may become a Contracting State, applies, including any of the conventions referred to in paragraph 1 of this article, even if such State has not excluded the application of paragraph 2 of this article by a declaration made in accordance with article 21.

Article 21
Procedure and effects of declarations
1. Declarations under article 17, paragraph 4, article 19, paragraphs 1 and 2, and article 20, paragraphs 2, 3 and 4, may be made at any time. Declarations made at the time of signature are subject to confirmation upon ratification, acceptance or approval.
2. Declarations and their confirmations are to be in writing and to be formally notified to the depositary.
3. A declaration takes effect simultaneously with the entry into force of this Convention in respect of the State concerned. However, a declaration of which the depositary receives formal notification after such entry into force takes effect on the first day of the month following the expiration of six months after the date of its receipt by the depositary.

4. Any State that makes a declaration under this Convention may modify or withdraw it at any time by a formal notification in writing addressed to the depositary. The modification or withdrawal is to take effect on the first day of the month following the expiration of six months after the date of the receipt of the notification by the depositary.

Article 22
Reservations
No reservations may be made under this Convention.

Article 23
Entry into force
1. This Convention enters into force on the first day of the month following the expiration of six months after the date of deposit of the third instrument of ratification, acceptance, approval or accession.
2. When a State ratifies, accepts, approves or accedes to this Convention after the deposit of the third instrument of ratification, acceptance, approval or accession, this Convention enters into force in respect of that State on the first day of the month following the expiration of six months after the date of the deposit of its instrument of ratification, acceptance, approval or accession.

Article 24
Time of application
This Convention and any declaration apply only to electronic communications that are made after the date when the Convention or the declaration enters into force or takes effect in respect of each Contracting State.

Article 25
Denunciations
1. A Contracting State may denounce this Convention by a formal notification in writing addressed to the depositary.
2. The denunciation takes effect on the first day of the month following the expiration of twelve months after the notification is received by the depositary.
Where a longer period for the denunciation to take effect is specified in the notification, the denunciation takes effect upon the expiration of such longer period after the notification is received by the depositary.

Appendix 2

UNITED NATIONS CONVENTION ON CONTRACTS FOR THE INTERNATIONAL CARRIAGE OF GOODS WHOLLY OR PARTLY BY SEA

UNITED NATIONS
2008

UNITED NATIONS CONVENTION ON CONTRACTS FOR THE INTERNATIONAL CARRIAGE OF GOODS WHOLLY OR PARTLY BY SEA

The States Parties to this Convention,

Reaffirming their belief that international trade on the basis of equality and mutual benefit is an important element in promoting friendly relations among States,

Convinced that the progressive harmonization and unification of international trade law, in reducing or removing legal obstacles to the flow of international trade, significantly contributes to universal economic cooperation among all States on a basis of equality, equity and common interest, and to the well-being of all peoples,

Recognizing the significant contribution of the International Convention for the Unification of Certain Rules of Law relating to Bills of Lading, signed in Brussels on 25 August 1924, and its Protocols, and of the United Nations Convention on the Carriage of Goods by Sea, signed in Hamburg on 31 March 1978, to the harmonization of the law governing the carriage of goods by sea,

Mindful of the technological and commercial developments that have taken place since the adoption of those conventions and of the need to consolidate and modernize them,

Noting that shippers and carriers do not have the benefit of a binding universal regime to support the operation of contracts of maritime carriage involving other modes of transport,

Believing that the adoption of uniform rules to govern international contracts of carriage wholly or partly by sea will promote legal certainty, improve the efficiency of international carriage of goods and facilitate new access opportunities for previously remote parties and markets, thus playing a fundamental role in promoting trade and economic development, both domestically and internationally,

Have agreed as follows:

Chapter 1
General provisions

Article 1
Definitions

For the purposes of this Convention:

1. "Contract of carriage" means a contract in which a carrier, against the payment of freight, undertakes to carry goods from one place to another. The contract shall provide for carriage by sea and may provide for carriage by other modes of transport in addition to the sea carriage.

2. "Volume contract" means a contract of carriage that provides for the carriage of a specified quantity of goods in a series of shipments during an agreed period of time. The specification of the quantity may include a minimum, a maximum or a certain range.

3. "Liner transportation" means a transportation service that is offered to the public through publication or similar means and includes transportation by ships operating on a regular schedule between specified ports in accordance with publicly available timetables of sailing dates.

4. "Non-liner transportation" means any transportation that is not liner transportation.

5. "Carrier" means a person that enters into a contract of carriage with a shipper.

6. (*a*) "Performing party" means a person other than the carrier that performs or undertakes to perform any of the carrier's obligations under a contract of carriage with respect to the receipt, loading, handling, stowage, carriage, care, unloading or delivery of the goods, to the extent that such person acts, either directly or indirectly, at the carrier's request or under the carrier's supervision or control.

(*b*) "Performing party" does not include any person that is retained, directly or indirectly, by a shipper, by a documentary shipper, by the controlling party or by the consignee instead of by the carrier.

7. "Maritime performing party" means a performing party to the extent that it performs or undertakes to perform any of the carrier's obligations during the period between the arrival of the goods at the port of loading of a ship and their departure from the port of discharge of a ship. An inland carrier is a maritime performing party only if it performs or undertakes to perform its services exclusively within a port area.

8. "Shipper" means a person that enters into a contract of carriage with a carrier.

9. "Documentary shipper" means a person, other than the shipper, that accepts to be named as "shipper" in the transport document or electronic transport record.

10. "Holder" means:

(*a*) A person that is in possession of a negotiable transport document; and (i) if the document is an order document, is identified in it as the shipper or the consignee, or is the person to which the document is duly endorsed; or (ii) if the document is a blank endorsed order document or bearer document, is the bearer thereof; or

(*b*) The person to which a negotiable electronic transport record has been issued or transferred in accordance with the procedures referred to in article 9, paragraph 1.

11. "Consignee" means a person entitled to delivery of the goods under a contract of carriage or a transport document or electronic transport record.

12. "Right of control" of the goods means the right under the contract of carriage to give the carrier instructions in respect of the goods in accordance with chapter 10.

13. "Controlling party" means the person that pursuant to article 51 is entitled to exercise the right of control.

14. "Transport document" means a document issued under a contract of carriage by the carrier that:

(*a*) Evidences the carrier's or a performing party's receipt of goods under a contract of carriage; and

(*b*) Evidences or contains a contract of carriage.

15. "Negotiable transport document" means a transport document that indicates, by wording such as "to order" or "negotiable" or other appropriate

wording recognized as having the same effect by the law applicable to the document, that the goods have been consigned to the order of the shipper, to the order of the consignee, or to bearer, and is not explicitly stated as being "non-negotiable" or "not negotiable".

16. "Non-negotiable transport document" means a transport document that is not a negotiable transport document.

17. "Electronic communication" means information generated, sent, received or stored by electronic, optical, digital or similar means with the result that the information communicated is accessible so as to be usable for subsequent reference.

18. "Electronic transport record" means information in one or more messages issued by electronic communication under a contract of carriage by a carrier, including information logically associated with the electronic transport record by attachments or otherwise linked to the electronic transport record contemporaneously with or subsequent to its issue by the carrier, so as to become part of the electronic transport record, that:

(*a*) Evidences the carrier's or a performing party's receipt of goods under a contract of carriage; and

(*b*) Evidences or contains a contract of carriage.

19. "Negotiable electronic transport record" means an electronic transport record:

(*a*) That indicates, by wording such as "to order", or "negotiable", or other appropriate wording recognized as having the same effect by the law applicable to the record, that the goods have been consigned to the order of the shipper or to the order of the consignee, and is not explicitly stated as being "non-negotiable" or "not negotiable"; and

(*b*) The use of which meets the requirements of article 9, paragraph 1.

20. "Non-negotiable electronic transport record" means an electronic transport record that is not a negotiable electronic transport record.

21. The "issuance" of a negotiable electronic transport record means the issuance of the record in accordance with procedures that ensure that the record is subject to exclusive control from its creation until it ceases to have any effect or validity.

22. The "transfer" of a negotiable electronic transport record means the transfer of exclusive control over the record.

23. "Contract particulars" means any information relating to the contract of carriage or to the goods (including terms, notations, signatures and endorsements) that is in a transport document or an electronic transport record.

24. "Goods" means the wares, merchandise, and articles of every kind whatsoever that a carrier undertakes to carry under a contract of carriage and includes the packing and any equipment and container not supplied by or on behalf of the carrier.

25. "Ship" means any vessel used to carry goods by sea.

26. "Container" means any type of container, transportable tank or flat, swapbody, or any similar unit load used to consolidate goods, and any equipment ancillary to such unit load.

27. "Vehicle" means a road or railroad cargo vehicle.

28. "Freight" means the remuneration payable to the carrier for the carriage of goods under a contract of carriage.

29. "Domicile" means (*a*) a place where a company or other legal person or association of natural or legal persons has its (i) statutory seat or place of incorporation or central registered office, whichever is applicable, (ii) central administration or (iii) principal place of business, and (*b*) the habitual residence of a natural person.

30. "Competent court" means a court in a Contracting State that, according to the rules on the internal allocation of jurisdiction among the courts of that State, may exercise jurisdiction over the dispute.

Article 2
Interpretation of this Convention

In the interpretation of this Convention, regard is to be had to its international character and to the need to promote uniformity in its application and the observance of good faith in international trade.

Article 3
Form requirements

The notices, confirmation, consent, agreement, declaration and other communications referred to in articles 19, paragraph 2; 23, paragraphs 1 to 4; 36, subparagraphs 1 (*b*), (*c*) and (*d*); 40, subparagraph 4 (*b*); 44; 48, paragraph 3; 51, subparagraph 1 (*b*); 59, paragraph 1; 63; 66; 67, paragraph 2; 75, paragraph 4; and 80, paragraphs 2 and 5, shall be in writing. Electronic communications

may be used for these purposes, provided that the use of such means is with the consent of the person by which it is communicated and of the person to which it is communicated.

Article 4
Applicability of defences and limits of liability

1. Any provision of this Convention that may provide a defence for, or limit the liability of, the carrier applies in any judicial or arbitral proceeding, whether founded in contract, in tort, or otherwise, that is instituted in respect of loss of, damage to, or delay in delivery of goods covered by a contract of carriage or for the breach of any other obligation under this Convention against:

(*a*) The carrier or a maritime performing party;

(*b*) The master, crew or any other person that performs services on board the ship; or

(*c*) Employees of the carrier or a maritime performing party.

2. Any provision of this Convention that may provide a defence for the shipper or the documentary shipper applies in any judicial or arbitral proceeding, whether founded in contract, in tort, or otherwise, that is instituted against the shipper, the documentary shipper, or their subcontractors, agents or employees.

Chapter 2
Scope of application

Article 5
General scope of application

1. Subject to article 6, this Convention applies to contracts of carriage in which the place of receipt and the place of delivery are in different States, and the port of loading of a sea carriage and the port of discharge of the same sea carriage are in different States, if, according to the contract of carriage, any one of the following places is located in a Contracting State:

(*a*) The place of receipt;

(*b*) The port of loading;

(*c*) The place of delivery; or

(*d*) The port of discharge.

2. This Convention applies without regard to the nationality of the vessel, the carrier, the performing parties, the shipper, the consignee, or any other interested parties.

Article 6
Specific exclusions

1. This Convention does not apply to the following contracts in liner transportation:

(*a*) Charter parties; and

(*b*) Other contracts for the use of a ship or of any space thereon.

2. This Convention does not apply to contracts of carriage in non-liner transportation except when:

(*a*) There is no charter party or other contract between the parties for the use of a ship or of any space thereon; and

(*b*) A transport document or an electronic transport record is issued.

Article 7
Application to certain parties

Notwithstanding article 6, this Convention applies as between the carrier and the consignee, controlling party or holder that is not an original party to the charter party or other contract of carriage excluded from the application of this Convention. However, this Convention does not apply as between the original parties to a contract of carriage excluded pursuant to article 6.

Chapter 3
Electronic transport records

Article 8
Use and effect of electronic transport records

Subject to the requirements set out in this Convention:

(*a*) Anything that is to be in or on a transport document under this Convention may be recorded in an electronic transport record, provided the issuance and subsequent use of an electronic transport record is with the consent of the carrier and the shipper; and

(*b*) The issuance, exclusive control, or transfer of an electronic transport record has the same effect as the issuance, possession, or transfer of a transport document.

Article 9
Procedures for use of negotiable electronic transport records

1. The use of a negotiable electronic transport record shall be subject to procedures that provide for:

(*a*) The method for the issuance and the transfer of that record to an intended holder;

(*b*) An assurance that the negotiable electronic transport record retains its integrity;

(*c*) The manner in which the holder is able to demonstrate that it is the holder; and

(*d*) The manner of providing confirmation that delivery to the holder has been effected, or that, pursuant to articles 10, paragraph 2, or 47, subparagraphs 1 (*a*) (ii) and (*c*), the electronic transport record has ceased to have any effect or validity.

2. The procedures in paragraph 1 of this article shall be referred to in the contract particulars and be readily ascertainable.

Article 10
Replacement of negotiable transport document or negotiable electronic transport record

1. If a negotiable transport document has been issued and the carrier and the holder agree to replace that document by a negotiable electronic transport record:

(*a*) The holder shall surrender the negotiable transport document, or all of them if more than one has been issued, to the carrier;

(*b*) The carrier shall issue to the holder a negotiable electronic transport record that includes a statement that it replaces the negotiable transport document; and

(*c*) The negotiable transport document ceases thereafter to have any effect or validity.

2. If a negotiable electronic transport record has been issued and the carrier and the holder agree to replace that electronic transport record by a negotiable transport document:

(*a*) The carrier shall issue to the holder, in place of the electronic transport record, a negotiable transport document that includes a statement that it replaces the negotiable electronic transport record; and

(*b*) The electronic transport record ceases thereafter to have any effect or validity.

Chapter 4
Obligations of the carrier

Article 11
Carriage and delivery of the goods

The carrier shall, subject to this Convention and in accordance with the terms of the contract of carriage, carry the goods to the place of destination and deliver them to the consignee.

Article 12
Period of responsibility of the carrier

1. The period of responsibility of the carrier for the goods under this Convention begins when the carrier or a performing party receives the goods for carriage and ends when the goods are delivered.

2. (*a*) If the law or regulations of the place of receipt require the goods to be handed over to an authority or other third party from which the carrier may collect them, the period of responsibility of the carrier begins when the carrier collects the goods from the authority or other third party.

(*b*) If the law or regulations of the place of delivery require the carrier to hand over the goods to an authority or other third party from which the consignee may collect them, the period of responsibility of the carrier ends when the carrier hands the goods over to the authority or other third party.

3. For the purpose of determining the carrier's period of responsibility, the parties may agree on the time and location of receipt and delivery of the goods, but a provision in a contract of carriage is void to the extent that it provides that:

(*a*) The time of receipt of the goods is subsequent to the beginning of their initial loading under the contract of carriage; or

(*b*) The time of delivery of the goods is prior to the completion of their final unloading under the contract of carriage.

Article 13
Specific obligations

1. The carrier shall during the period of its responsibility as defined in article 12, and subject to article 26, properly and carefully receive, load, handle, stow, carry, keep, care for, unload and deliver the goods.

2. Notwithstanding paragraph 1 of this article, and without prejudice to the other provisions in chapter 4 and to chapters 5 to 7, the carrier and the shipper may agree that the loading, handling, stowing or unloading of the goods is to be performed by the shipper, the documentary shipper or the consignee. Such an agreement shall be referred to in the contract particulars.

Article 14
Specific obligations applicable to the voyage by sea

The carrier is bound before, at the beginning of, and during the voyage by sea to exercise due diligence to:

(*a*) Make and keep the ship seaworthy;

(*b*) Properly crew, equip and supply the ship and keep the ship so crewed, equipped and supplied throughout the voyage; and

(*c*) Make and keep the holds and all other parts of the ship in which the goods are carried, and any containers supplied by the carrier in or upon which the goods are carried, fit and safe for their reception, carriage and preservation.

Article 15
Goods that may become a danger

Notwithstanding articles 11 and 13, the carrier or a performing party may decline to receive or to load, and may take such other measures as are reasonable, including unloading, destroying, or rendering goods harmless, if the goods are, or reasonably appear likely to become during the carrier's period of responsibility, an actual danger to persons, property or the environment.

Article 16
Sacrifice of the goods during the voyage by sea

Notwithstanding articles 11, 13, and 14, the carrier or a performing party may sacrifice goods at sea when the sacrifice is reasonably made for the common safety or for the purpose of preserving from peril human life or other property involved in the common adventure.

Chapter 5
Liability of the carrier for loss, damage or delay

Article 17
Basis of liability

1. The carrier is liable for loss of or damage to the goods, as well as for delay in delivery, if the claimant proves that the loss, damage, or delay, or the event or circumstance that caused or contributed to it took place during the period of the carrier's responsibility as defined in chapter 4.

2. The carrier is relieved of all or part of its liability pursuant to paragraph 1 of this article if it proves that the cause or one of the causes of the loss, damage, or delay is not attributable to its fault or to the fault of any person referred to in article 18.

3. The carrier is also relieved of all or part of its liability pursuant to paragraph 1 of this article if, alternatively to proving the absence of fault as provided in paragraph 2 of this article, it proves that one or more of the following events or circumstances caused or contributed to the loss, damage, or delay:

(*a*) Act of God;

(*b*) Perils, dangers, and accidents of the sea or other navigable waters;

(*c*) War, hostilities, armed conflict, piracy, terrorism, riots, and civil commotions;

(*d*) Quarantine restrictions; interference by or impediments created by governments, public authorities, rulers, or people including detention, arrest, or seizure not attributable to the carrier or any person referred to in article 18;

(*e*) Strikes, lockouts, stoppages, or restraints of labour;

(*f*) Fire on the ship;

(*g*) Latent defects not discoverable by due diligence;

(*h*) Act or omission of the shipper, the documentary shipper, the controlling party, or any other person for whose acts the shipper or the documentary shipper is liable pursuant to article 33 or 34;

(*i*) Loading, handling, stowing, or unloading of the goods performed pursuant to an agreement in accordance with article 13, paragraph 2, unless the carrier or a performing party performs such activity on behalf of the shipper, the documentary shipper or the consignee;

(*j*) Wastage in bulk or weight or any other loss or damage arising from inherent defect, quality, or vice of the goods;

(*k*) Insufficiency or defective condition of packing or marking not performed by or on behalf of the carrier;

(*l*) Saving or attempting to save life at sea;

(*m*) Reasonable measures to save or attempt to save property at sea;

(*n*) Reasonable measures to avoid or attempt to avoid damage to the environment; or

(*o*) Acts of the carrier in pursuance of the powers conferred by articles 15 and 16.

4. Notwithstanding paragraph 3 of this article, the carrier is liable for all or part of the loss, damage, or delay:

(*a*) If the claimant proves that the fault of the carrier or of a person referred to in article 18 caused or contributed to the event or circumstance on which the carrier relies; or

(*b*) If the claimant proves that an event or circumstance not listed in paragraph 3 of this article contributed to the loss, damage, or delay, and the carrier cannot prove that this event or circumstance is not attributable to its fault or to the fault of any person referred to in article 18.

5. The carrier is also liable, notwithstanding paragraph 3 of this article, for all or part of the loss, damage, or delay if:

(*a*) The claimant proves that the loss, damage, or delay was or was probably caused by or contributed to by (i) the unseaworthiness of the ship; (ii) the improper crewing, equipping, and supplying of the ship; or (iii) the fact that the holds or other parts of the ship in which the goods are carried, or any containers supplied by the carrier in or upon which the goods are carried, were not fit and safe for reception, carriage, and preservation of the goods; and

(*b*) The carrier is unable to prove either that: (i) none of the events or circumstances referred to in subparagraph 5 (*a*) of this article caused the loss, damage, or delay; or (ii) it complied with its obligation to exercise due diligence pursuant to article 14.

6. When the carrier is relieved of part of its liability pursuant to this article, the carrier is liable only for that part of the loss, damage or delay that is attributable to the event or circumstance for which it is liable pursuant to this article.

Article 18
Liability of the carrier for other persons

The carrier is liable for the breach of its obligations under this Convention caused by the acts or omissions of:

(*a*) Any performing party;

(*b*) The master or crew of the ship;

(*c*) Employees of the carrier or a performing party; or

(*d*) Any other person that performs or undertakes to perform any of the carrier's obligations under the contract of carriage, to the extent that the person acts, either directly or indirectly, at the carrier's request or under the carrier's supervision or control.

Article 19
Liability of maritime performing parties

1. A maritime performing party is subject to the obligations and liabilities imposed on the carrier under this Convention and is entitled to the carrier's defences and limits of liability as provided for in this Convention if:

(*a*) The maritime performing party received the goods for carriage in a Contracting State, or delivered them in a Contracting State, or performed its activities with respect to the goods in a port in a Contracting State; and

(*b*) The occurrence that caused the loss, damage or delay took place: (i) during the period between the arrival of the goods at the port of loading of the ship and their departure from the port of discharge from the ship; (ii) while the maritime performing party had custody of the goods; or (iii) at any other time to the extent that it was participating in the performance of any of the activities contemplated by the contract of carriage.

2. If the carrier agrees to assume obligations other than those imposed on the carrier under this Convention, or agrees that the limits of its liability are higher than the limits specified under this Convention, a maritime performing party is not bound by this agreement unless it expressly agrees to accept such obligations or such higher limits.

3. A maritime performing party is liable for the breach of its obligations under this Convention caused by the acts or omissions of any person to which it has entrusted the performance of any of the carrier's obligations under the contract of carriage under the conditions set out in paragraph 1 of this article.

4. Nothing in this Convention imposes liability on the master or crew of the ship or on an employee of the carrier or of a maritime performing party.

Article 20
Joint and several liability

1. If the carrier and one or more maritime performing parties are liable for the loss of, damage to, or delay in delivery of the goods, their liability is joint and several but only up to the limits provided for under this Convention.

2. Without prejudice to article 61, the aggregate liability of all such persons shall not exceed the overall limits of liability under this Convention.

Article 21
Delay

Delay in delivery occurs when the goods are not delivered at the place of destination provided for in the contract of carriage within the time agreed.

Article 22
Calculation of compensation

1. Subject to article 59, the compensation payable by the carrier for loss of or damage to the goods is calculated by reference to the value of such goods at the place and time of delivery established in accordance with article 43.

2. The value of the goods is fixed according to the commodity exchange price or, if there is no such price, according to their market price or, if there is no commodity exchange price or market price, by reference to the normal value of the goods of the same kind and quality at the place of delivery.

3. In case of loss of or damage to the goods, the carrier is not liable for payment of any compensation beyond what is provided for in paragraphs 1 and 2 of this article except when the carrier and the shipper have agreed to calculate compensation in a different manner within the limits of chapter 16.

Article 23
Notice in case of loss, damage or delay

1. The carrier is presumed, in absence of proof to the contrary, to have delivered the goods according to their description in the contract particulars unless notice of loss of or damage to the goods, indicating the general nature of such loss or damage, was given to the carrier or the performing party that delivered the goods before or at the time of the delivery, or, if the loss or damage is not apparent, within seven working days at the place of delivery after the delivery of the goods.

2. Failure to provide the notice referred to in this article to the carrier or the performing party shall not affect the right to claim compensation for loss of or damage to the goods under this Convention, nor shall it affect the allocation of the burden of proof set out in article 17.

3. The notice referred to in this article is not required in respect of loss or damage that is ascertained in a joint inspection of the goods by the person to which they have been delivered and the carrier or the maritime performing party against which liability is being asserted.

4. No compensation in respect of delay is payable unless notice of loss due to delay was given to the carrier within twenty-one consecutive days of delivery of the goods.

5. When the notice referred to in this article is given to the performing party that delivered the goods, it has the same effect as if that notice was given to the carrier, and notice given to the carrier has the same effect as a notice given to a maritime performing party.

6. In the case of any actual or apprehended loss or damage, the parties to the dispute shall give all reasonable facilities to each other for inspecting and tallying the goods and shall provide access to records and documents relevant to the carriage of the goods.

Chapter 6
Additional provisions relating to particular stages of carriage

Article 24
Deviation

When pursuant to applicable law a deviation constitutes a breach of the carrier's obligations, such deviation of itself shall not deprive the carrier or a maritime performing party of any defence or limitation of this Convention, except to the extent provided in article 61.

Article 25
Deck cargo on ships

1. Goods may be carried on the deck of a ship only if:

(*a*) Such carriage is required by law;

(*b*) They are carried in or on containers or vehicles that are fit for deck carriage, and the decks are specially fitted to carry such containers or vehicles; or

(*c*) The carriage on deck is in accordance with the contract of carriage, or the customs, usages or practices of the trade in question.

2. The provisions of this Convention relating to the liability of the carrier apply to the loss of, damage to or delay in the delivery of goods carried on deck pursuant to paragraph 1 of this article, but the carrier is not liable for loss of or damage to such goods, or delay in their delivery, caused by the special risks involved in their carriage on deck when the goods are carried in accordance with subparagraphs 1 (*a*) or (*c*) of this article.

3. If the goods have been carried on deck in cases other than those permitted pursuant to paragraph 1 of this article, the carrier is liable for loss of or damage to the goods or delay in their delivery that is exclusively caused by their carriage on deck, and is not entitled to the defences provided for in article 17.

4. The carrier is not entitled to invoke subparagraph 1 (*c*) of this article against a third party that has acquired a negotiable transport document or a negotiable electronic transport record in good faith, unless the contract particulars state that the goods may be carried on deck.

5. If the carrier and shipper expressly agreed that the goods would be carried under deck, the carrier is not entitled to the benefit of the limitation of liability for any loss of, damage to or delay in the delivery of the goods to the extent that such loss, damage, or delay resulted from their carriage on deck.

Article 26
Carriage preceding or subsequent to sea carriage

When loss of or damage to goods, or an event or circumstance causing a delay in their delivery, occurs during the carrier's period of responsibility but solely before their loading onto the ship or solely after their discharge from the ship, the provisions of this Convention do not prevail over those provisions of another international instrument that, at the time of such loss, damage or event or circumstance causing delay:

(*a*) Pursuant to the provisions of such international instrument would have applied to all or any of the carrier's activities if the shipper had made a separate and direct contract with the carrier in respect of the particular stage of carriage where the loss of, or damage to goods, or an event or circumstance causing delay in their delivery occurred;

(*b*) Specifically provide for the carrier's liability, limitation of liability, or time for suit; and

(*c*) Cannot be departed from by contract either at all or to the detriment of the shipper under that instrument.

Chapter 7
Obligations of the shipper to the carrier

Article 27
Delivery for carriage

1. Unless otherwise agreed in the contract of carriage, the shipper shall deliver the goods ready for carriage. In any event, the shipper shall deliver the goods in such condition that they will withstand the intended carriage, including their loading, handling, stowing, lashing and securing, and unloading, and that they will not cause harm to persons or property.

2. The shipper shall properly and carefully perform any obligation assumed under an agreement made pursuant to article 13, paragraph 2.

3. When a container is packed or a vehicle is loaded by the shipper, the shipper shall properly and carefully stow, lash and secure the contents in or on the container or vehicle, and in such a way that they will not cause harm to persons or property.

Article 28
Cooperation of the shipper and the carrier in providing information and instructions

The carrier and the shipper shall respond to requests from each other to provide information and instructions required for the proper handling and carriage of the goods if the information is in the requested party's possession or the instructions are within the requested party's reasonable ability to provide and they are not otherwise reasonably available to the requesting party.

Article 29
Shipper's obligation to provide information, instructions and documents

1. The shipper shall provide to the carrier in a timely manner such information, instructions and documents relating to the goods that are not otherwise reasonably available to the carrier, and that are reasonably necessary:

(*a*) For the proper handling and carriage of the goods, including precautions to be taken by the carrier or a performing party; and

(*b*) For the carrier to comply with law, regulations or other requirements of public authorities in connection with the intended carriage, provided that the carrier notifies the shipper in a timely manner of the information, instructions and documents it requires.

2. Nothing in this article affects any specific obligation to provide certain information, instructions and documents related to the goods pursuant to law, regulations or other requirements of public authorities in connection with the intended carriage.

Article 30
Basis of shipper's liability to the carrier

1. The shipper is liable for loss or damage sustained by the carrier if the carrier proves that such loss or damage was caused by a breach of the shipper's obligations under this Convention.

2. Except in respect of loss or damage caused by a breach by the shipper of its obligations pursuant to articles 31, paragraph 2, and 32, the shipper is relieved of all or part of its liability if the cause or one of the causes of the loss or damage is not attributable to its fault or to the fault of any person referred to in article 34.

3. When the shipper is relieved of part of its liability pursuant to this article, the shipper is liable only for that part of the loss or damage that is attributable to its fault or to the fault of any person referred to in article 34.

Article 31
Information for compilation of contract particulars

1. The shipper shall provide to the carrier, in a timely manner, accurate information required for the compilation of the contract particulars and the issuance of the transport documents or electronic transport records, including the particulars referred to in article 36, paragraph 1; the name of the party to be identified as the shipper in the contract particulars; the name of the consignee, if any; and the name of the person to whose order the transport document or electronic transport record is to be issued, if any.

2. The shipper is deemed to have guaranteed the accuracy at the time of receipt by the carrier of the information that is provided according to paragraph 1 of this article. The shipper shall indemnify the carrier against loss or damage resulting from the inaccuracy of such information.

Article 32
Special rules on dangerous goods

When goods by their nature or character are, or reasonably appear likely to become, a danger to persons, property or the environment:

(*a*) The shipper shall inform the carrier of the dangerous nature or character of the goods in a timely manner before they are delivered to the carrier or a performing party. If the shipper fails to do so and the carrier or performing party does not otherwise have knowledge of their dangerous nature or character, the shipper is liable to the carrier for loss or damage resulting from such failure to inform; and

(*b*) The shipper shall mark or label dangerous goods in accordance with any law, regulations or other requirements of public authorities that apply during any stage of the intended carriage of the goods. If the shipper fails to do so, it is liable to the carrier for loss or damage resulting from such failure.

Article 33
Assumption of shipper's rights and obligations by the documentary shipper

1. A documentary shipper is subject to the obligations and liabilities imposed on the shipper pursuant to this chapter and pursuant to article 55, and is entitled to the shipper's rights and defences provided by this chapter and by chapter 13.

2. Paragraph 1 of this article does not affect the obligations, liabilities, rights or defences of the shipper.

Article 34
Liability of the shipper for other persons

The shipper is liable for the breach of its obligations under this Convention caused by the acts or omissions of any person, including employees, agents and subcontractors, to which it has entrusted the performance of any of its obligations, but the shipper is not liable for acts or omissions of the carrier or a performing party acting on behalf of the carrier, to which the shipper has entrusted the performance of its obligations.

Chapter 8
Transport documents and electronic transport records

Article 35
Issuance of the transport document or the electronic transport record

Unless the shipper and the carrier have agreed not to use a transport document or an electronic transport record, or it is the custom, usage or practice of the trade not to use one, upon delivery of the goods for carriage to the carrier or performing party, the shipper or, if the shipper consents, the documentary shipper, is entitled to obtain from the carrier, at the shipper's option:

(*a*) A non-negotiable transport document or, subject to article 8, subparagraph (*a*), a non-negotiable electronic transport record; or

(*b*) An appropriate negotiable transport document or, subject to article 8, subparagraph (*a*), a negotiable electronic transport record, unless the shipper and the carrier have agreed not to use a negotiable transport document or negotiable electronic transport record, or it is the custom, usage or practice of the trade not to use one.

Article 36
Contract particulars

1. The contract particulars in the transport document or electronic transport record referred to in article 35 shall include the following information, as furnished by the shipper:

(*a*) A description of the goods as appropriate for the transport;

(*b*) The leading marks necessary for identification of the goods;

(*c*) The number of packages or pieces, or the quantity of goods; and

(*d*) The weight of the goods, if furnished by the shipper.

2. The contract particulars in the transport document or electronic transport record referred to in article 35 shall also include:

(*a*) A statement of the apparent order and condition of the goods at the time the carrier or a performing party receives them for carriage;

(*b*) The name and address of the carrier;

(*c*) The date on which the carrier or a performing party received the goods, or on which the goods were loaded on board the ship, or on which the transport document or electronic transport record was issued; and

(*d*) If the transport document is negotiable, the number of originals of the negotiable transport document, when more than one original is issued.

3. The contract particulars in the transport document or electronic transport record referred to in article 35 shall further include:

(*a*) The name and address of the consignee, if named by the shipper;

(*b*) The name of a ship, if specified in the contract of carriage;

(*c*) The place of receipt and, if known to the carrier, the place of delivery; and

(*d*) The port of loading and the port of discharge, if specified in the contract of carriage.

4. For the purposes of this article, the phrase "apparent order and condition of the goods" in subparagraph 2 (*a*) of this article refers to the order and condition of the goods based on:

(*a*) A reasonable external inspection of the goods as packaged at the time the shipper delivers them to the carrier or a performing party; and

(*b*) Any additional inspection that the carrier or a performing party actually performs before issuing the transport document or electronic transport record.

Article 37
Identity of the carrier

1. If a carrier is identified by name in the contract particulars, any other information in the transport document or electronic transport record relating to the identity of the carrier shall have no effect to the extent that it is inconsistent with that identification.

2. If no person is identified in the contract particulars as the carrier as required pursuant to article 36, subparagraph 2 (*b*), but the contract particulars indicate that the goods have been loaded on board a named ship, the registered owner of that ship is presumed to be the carrier, unless it proves that the ship was under a bareboat charter at the time of the carriage and it identifies this bareboat charterer and indicates its address, in which case this bareboat charterer is presumed to be the carrier. Alternatively, the registered owner may rebut the presumption of being the carrier by identifying the carrier and indicating its address. The bareboat charterer may rebut any presumption of being the carrier in the same manner.

3. Nothing in this article prevents the claimant from proving that any person other than a person identified in the contract particulars or pursuant to paragraph 2 of this article is the carrier.

Article 38
Signature

1. A transport document shall be signed by the carrier or a person acting on its behalf.

2. An electronic transport record shall include the electronic signature of the carrier or a person acting on its behalf. Such electronic signature shall identify the signatory in relation to the electronic transport record and indicate the carrier's authorization of the electronic transport record.

Article 39
Deficiencies in the contract particulars

1. The absence or inaccuracy of one or more of the contract particulars referred to in article 36, paragraphs 1, 2 or 3, does not of itself affect the legal character or validity of the transport document or of the electronic transport record.

2. If the contract particulars include the date but fail to indicate its significance, the date is deemed to be:

(*a*) The date on which all of the goods indicated in the transport document or electronic transport record were loaded on board the ship, if the contract particulars indicate that the goods have been loaded on board a ship; or

(*b*) The date on which the carrier or a performing party received the goods, if the contract particulars do not indicate that the goods have been loaded on board a ship.

3. If the contract particulars fail to state the apparent order and condition of the goods at the time the carrier or a performing party receives them, the contract particulars are deemed to have stated that the goods were in apparent good order and condition at the time the carrier or a performing party received them.

Article 40
Qualifying the information relating to the goods in the contract particulars

1. The carrier shall qualify the information referred to in article 36, paragraph 1, to indicate that the carrier does not assume responsibility for the accuracy of the information furnished by the shipper if:

(*a*) The carrier has actual knowledge that any material statement in the transport document or electronic transport record is false or misleading; or

(*b*) The carrier has reasonable grounds to believe that a material statement in the transport document or electronic transport record is false or misleading.

2. Without prejudice to paragraph 1 of this article, the carrier may qualify the information referred to in article 36, paragraph 1, in the circumstances and in the manner set out in paragraphs 3 and 4 of this article to indicate that the carrier does not assume responsibility for the accuracy of the information furnished by the shipper.

3. When the goods are not delivered for carriage to the carrier or a performing party in a closed container or vehicle, or when they are delivered in a closed container or vehicle and the carrier or a performing party actually inspects them, the carrier may qualify the information referred to in article 36, paragraph 1, if:

(*a*) The carrier had no physically practicable or commercially reasonable means of checking the information furnished by the shipper, in which case it may indicate which information it was unable to check; or

(*b*) The carrier has reasonable grounds to believe the information furnished by the shipper to be inaccurate, in which case it may include a clause providing what it reasonably considers accurate information.

4. When the goods are delivered for carriage to the carrier or a performing party in a closed container or vehicle, the carrier may qualify the information referred to in:

(*a*) Article 36, subparagraphs 1 (*a*), (*b*), or (*c*), if:

(i) The goods inside the container or vehicle have not actually been inspected by the carrier or a performing party; and

(ii) Neither the carrier nor a performing party otherwise has actual knowledge of its contents before issuing the transport document or the electronic transport record; and

(*b*) Article 36, subparagraph 1 (*d*), if:

(i) Neither the carrier nor a performing party weighed the container or vehicle, and the shipper and the carrier had not agreed prior to the shipment that the container or vehicle would be weighed and the weight would be included in the contract particulars; or

(ii) There was no physically practicable or commercially reasonable means of checking the weight of the container or vehicle.

Article 41
Evidentiary effect of the contract particulars

Except to the extent that the contract particulars have been qualified in the circumstances and in the manner set out in article 40:

(*a*) A transport document or an electronic transport record is prima facie evidence of the carrier's receipt of the goods as stated in the contract particulars;

(*b*) Proof to the contrary by the carrier in respect of any contract particulars shall not be admissible, when such contract particulars are included in:

(i) A negotiable transport document or a negotiable electronic transport record that is transferred to a third party acting in good faith; or

(ii) A non-negotiable transport document that indicates that it must be surrendered in order to obtain delivery of the goods and is transferred to the consignee acting in good faith;

(*c*) Proof to the contrary by the carrier shall not be admissible against a consignee that in good faith has acted in reliance on any of the following contract particulars included in a non-negotiable transport document or a non negotiable electronic transport record:

(i) The contract particulars referred to in article 36, paragraph 1, when such contract particulars are furnished by the carrier;

(ii) The number, type and identifying numbers of the containers, but not the identifying numbers of the container seals; and

(iii) The contract particulars referred to in article 36, paragraph 2.

Article 42
"Freight prepaid"

If the contract particulars contain the statement "freight prepaid" or a statement of a similar nature, the carrier cannot assert against the holder or the consignee the fact that the freight has not been paid. This article does not apply if the holder or the consignee is also the shipper.

Chapter 9
Delivery of the goods

Article 43
Obligation to accept delivery

When the goods have arrived at their destination, the consignee that demands delivery of the goods under the contract of carriage shall accept delivery of the goods at the time or within the time period and at the location agreed in the contract of carriage or, failing such agreement, at the time and location at which, having regard to the terms of the contract, the customs, usages or practices of the trade and the circumstances of the carriage, delivery could reasonably be expected.

Article 44
Obligation to acknowledge receipt

On request of the carrier or the performing party that delivers the goods, the consignee shall acknowledge receipt of the goods from the carrier or the performing party in the manner that is customary at the place of delivery. The carrier may refuse delivery if the consignee refuses to acknowledge such receipt.

Article 45
Delivery when no negotiable transport document or negotiable electronic transport record is issued

When neither a negotiable transport document nor a negotiable electronic transport record has been issued:

(*a*) The carrier shall deliver the goods to the consignee at the time and location referred to in article 43. The carrier may refuse delivery if the person claiming to be the consignee does not properly identify itself as the consignee on the request of the carrier;

(*b*) If the name and address of the consignee are not referred to in the contract particulars, the controlling party shall prior to or upon the arrival of the goods at the place of destination advise the carrier of such name and address;

(*c*) Without prejudice to article 48, paragraph 1, if the goods are not deliverable because (i) the consignee, after having received a notice of arrival, does not, at the time or within the time period referred to in article 43, claim delivery of the goods from the carrier after their arrival at the place of destination, (ii) the carrier refuses delivery because the person claiming to be the consignee does not properly identify itself as the consignee, or (iii) the carrier is, after reasonable effort, unable to locate the consignee in order to request delivery instructions, the carrier may so advise the controlling party and request instructions in respect of the delivery of the goods. If, after reasonable effort, the carrier is unable to locate the controlling party, the carrier may so advise the shipper and request instructions in respect of the delivery of the goods. If, after reasonable effort, the carrier is unable to locate the shipper, the carrier may so advise the documentary shipper and request instructions in respect of the delivery of the goods;

(*d*) The carrier that delivers the goods upon instruction of the controlling party, the shipper or the documentary shipper pursuant to subparagraph (*c*) of this article is discharged from its obligations to deliver the goods under the contract of carriage.

Article 46
Delivery when a non-negotiable transport document that requires surrender is issued

When a non-negotiable transport document has been issued that indicates that it shall be surrendered in order to obtain delivery of the goods:

(*a*) The carrier shall deliver the goods at the time and location referred to in article 43 to the consignee upon the consignee properly identifying itself on the request of the carrier and surrender of the non-negotiable document. The carrier may refuse delivery if the person claiming to be the consignee fails to properly identify itself on the request of the carrier, and shall refuse delivery if the non-negotiable document is not surrendered. If more than one original of the non-negotiable document has been issued, the surrender of one original will suffice and the other originals cease to have any effect or validity;

(*b*) Without prejudice to article 48, paragraph 1, if the goods are not deliverable because (i) the consignee, after having received a notice of arrival, does not, at the time or within the time period referred to in article 43, claim delivery of the goods from the carrier after their arrival at the place of destination, (ii) the carrier refuses delivery because the person claiming to be the consignee does not properly identify itself as the consignee or does not surrender the document, or (iii) the carrier is, after reasonable effort, unable to locate the consignee in order to request delivery instructions, the carrier may so advise the shipper and request instructions in respect of the delivery of the goods. If, after reasonable effort, the carrier is unable to locate the shipper, the carrier may so advise the documentary shipper and request instructions in respect of the delivery of the goods;

(*c*) The carrier that delivers the goods upon instruction of the shipper or the documentary shipper pursuant to subparagraph (*b*) of this article is discharged from its obligation to deliver the goods under the contract of carriage, irrespective of whether the non-negotiable transport document has been surrendered to it.

Article 47
Delivery when a negotiable transport document or negotiable electronic transport record is issued

1. When a negotiable transport document or a negotiable electronic transport record has been issued:

(*a*) The holder of the negotiable transport document or negotiable electronic transport record is entitled to claim delivery of the goods from the

carrier after they have arrived at the place of destination, in which event the carrier shall deliver the goods at the time and location referred to in article 43 to the holder:

(i) Upon surrender of the negotiable transport document and, if the holder is one of the persons referred to in article 1, subparagraph 10 (*a*) (i), upon the holder properly identifying itself; or

(ii) Upon demonstration by the holder, in accordance with the procedures referred to in article 9, paragraph 1, that it is the holder of the negotiable electronic transport record;

(*b*) The carrier shall refuse delivery if the requirements of subparagraph (*a*) (i) or (*a*) (ii) of this paragraph are not met;

(*c*) If more than one original of the negotiable transport document has been issued, and the number of originals is stated in that document, the surrender of one original will suffice and the other originals cease to have any effect or validity. When a negotiable electronic transport record has been used, such electronic transport record ceases to have any effect or validity upon delivery to the holder in accordance with the procedures required by article 9, paragraph 1.

2. Without prejudice to article 48, paragraph 1, if the negotiable transport document or the negotiable electronic transport record expressly states that the goods may be delivered without the surrender of the transport document or the electronic transport record, the following rules apply:

(*a*) If the goods are not deliverable because (i) the holder, after having received a notice of arrival, does not, at the time or within the time period referred to in article 43, claim delivery of the goods from the carrier after their arrival at the place of destination, (ii) the carrier refuses delivery because the person claiming to be a holder does not properly identify itself as one of the persons referred to in article 1, subparagraph 10 (*a*) (i), or (iii) the carrier is, after reasonable effort, unable to locate the holder in order to request delivery instructions, the carrier may so advise the shipper and request instructions in respect of the delivery of the goods. If, after reasonable effort, the carrier is unable to locate the shipper, the carrier may so advise the documentary shipper and request instructions in respect of the delivery of the goods;

(*b*) The carrier that delivers the goods upon instruction of the shipper or the documentary shipper in accordance with subparagraph 2 (*a*) of this article is discharged from its obligation to deliver the goods under the contract of carriage to the holder, irrespective of whether the negotiable transport document has been surrendered to it, or the person claiming delivery under a negotiable

electronic transport record has demonstrated, in accordance with the procedures referred to in article 9, paragraph 1, that it is the holder;

(*c*) The person giving instructions under subparagraph 2 (*a*) of this article shall indemnify the carrier against loss arising from its being held liable to the holder under subparagraph 2 (*e*) of this article. The carrier may refuse to follow those instructions if the person fails to provide adequate security as the carrier may reasonably request;

(*d*) A person that becomes a holder of the negotiable transport document or the negotiable electronic transport record after the carrier has delivered the goods pursuant to subparagraph 2 (*b*) of this article, but pursuant to contractual or other arrangements made before such delivery acquires rights against the carrier under the contract of carriage, other than the right to claim delivery of the goods;

(*e*) Notwithstanding subparagraphs 2 (*b*) and 2 (*d*) of this article, a holder that becomes a holder after such delivery, and that did not have and could not reasonably have had knowledge of such delivery at the time it became a holder, acquires the rights incorporated in the negotiable transport document or negotiable electronic transport record. When the contract particulars state the expected time of arrival of the goods, or indicate how to obtain information as to whether the goods have been delivered, it is presumed that the holder at the time that it became a holder had or could reasonably have had knowledge of the delivery of the goods.

Article 48
Goods remaining undelivered

1. For the purposes of this article, goods shall be deemed to have remained undelivered only if, after their arrival at the place of destination:

(*a*) The consignee does not accept delivery of the goods pursuant to this chapter at the time and location referred to in article 43;

(*b*) The controlling party, the holder, the shipper or the documentary shipper cannot be found or does not give the carrier adequate instructions pursuant to articles 45, 46 and 47;

(*c*) The carrier is entitled or required to refuse delivery pursuant to articles 44, 45, 46 and 47;

(*d*) The carrier is not allowed to deliver the goods to the consignee pursuant to the law or regulations of the place at which delivery is requested; or

(*e*) The goods are otherwise undeliverable by the carrier.

2. Without prejudice to any other rights that the carrier may have against the shipper, controlling party or consignee, if the goods have remained undelivered, the carrier may, at the risk and expense of the person entitled to the goods, take such action in respect of the goods as circumstances may reasonably require, including:

(*a*) To store the goods at any suitable place;

(*b*) To unpack the goods if they are packed in containers or vehicles, or to act otherwise in respect of the goods, including by moving them; and

(*c*) To cause the goods to be sold or destroyed in accordance with the practices or pursuant to the law or regulations of the place where the goods are located at the time.

3. The carrier may exercise the rights under paragraph 2 of this article only after it has given reasonable notice of the intended action under paragraph 2 of this article to the person stated in the contract particulars as the person, if any, to be notified of the arrival of the goods at the place of destination, and to one of the following persons in the order indicated, if known to the carrier: the consignee, the controlling party or the shipper.

4. If the goods are sold pursuant to subparagraph 2 (*c*) of this article, the carrier shall hold the proceeds of the sale for the benefit of the person entitled to the goods, subject to the deduction of any costs incurred by the carrier and any other amounts that are due to the carrier in connection with the carriage of those goods.

5. The carrier shall not be liable for loss of or damage to goods that occurs during the time that they remain undelivered pursuant to this article unless the claimant proves that such loss or damage resulted from the failure by the carrier to take steps that would have been reasonable in the circumstances to preserve the goods and that the carrier knew or ought to have known that the loss or damage to the goods would result from its failure to take such steps.

Article 49
Retention of goods

Nothing in this Convention affects a right of the carrier or a performing party that may exist pursuant to the contract of carriage or the applicable law to retain the goods to secure the payment of sums due.

Chapter 10
Rights of the controlling party

Article 50
Exercise and extent of right of control

1. The right of control may be exercised only by the controlling party and is limited to:

(*a*) The right to give or modify instructions in respect of the goods that do not constitute a variation of the contract of carriage;

(*b*) The right to obtain delivery of the goods at a scheduled port of call or, in respect of inland carriage, any place en route; and

(*c*) The right to replace the consignee by any other person including the controlling party.

2. The right of control exists during the entire period of responsibility of the carrier, as provided in article 12, and ceases when that period expires.

Article 51
Identity of the controlling party and transfer of the right of control

1. Except in the cases referred to in paragraphs 2, 3 and 4 of this article:

(*a*) The shipper is the controlling party unless the shipper, when the contract of carriage is concluded, designates the consignee, the documentary shipper or another person as the controlling party;

(*b*) The controlling party is entitled to transfer the right of control to another person. The transfer becomes effective with respect to the carrier upon its notification of the transfer by the transferor, and the transferee becomes the controlling party; and

(*c*) The controlling party shall properly identify itself when it exercises the right of control.

2. When a non-negotiable transport document has been issued that indicates that it shall be surrendered in order to obtain delivery of the goods:

(*a*) The shipper is the controlling party and may transfer the right of control to the consignee named in the transport document by transferring the

document to that person without endorsement. If more than one original of the document was issued, all originals shall be transferred in order to effect a transfer of the right of control; and

(*b*) In order to exercise its right of control, the controlling party shall produce the document and properly identify itself. If more than one original of the document was issued, all originals shall be produced, failing which the right of control cannot be exercised.

3. When a negotiable transport document is issued:

(*a*) The holder or, if more than one original of the negotiable transport document is issued, the holder of all originals is the controlling party;

(*b*) The holder may transfer the right of control by transferring the negotiable transport document to another person in accordance with article 57. If more than one original of that document was issued, all originals shall be transferred to that person in order to effect a transfer of the right of control; and

(*c*) In order to exercise the right of control, the holder shall produce the negotiable transport document to the carrier, and if the holder is one of the persons referred to in article 1, subparagraph 10 (*a*) (i), the holder shall properly identify itself. If more than one original of the document was issued, all originals shall be produced, failing which the right of control cannot be exercised.

4. When a negotiable electronic transport record is issued:

(*a*) The holder is the controlling party;

(*b*) The holder may transfer the right of control to another person by transferring the negotiable electronic transport record in accordance with the procedures referred to in article 9, paragraph 1; and

(*c*) In order to exercise the right of control, the holder shall demonstrate, in accordance with the procedures referred to in article 9, paragraph 1, that it is the holder.

Article 52
Carrier's execution of instructions

1. Subject to paragraphs 2 and 3 of this article, the carrier shall execute the instructions referred to in article 50 if:

(*a*) The person giving such instructions is entitled to exercise the right of control;

(*b*) The instructions can reasonably be executed according to their terms at the moment that they reach the carrier; and

(*c*) The instructions will not interfere with the normal operations of the carrier, including its delivery practices.

2. In any event, the controlling party shall reimburse the carrier for any reasonable additional expense that the carrier may incur and shall indemnify the carrier against loss or damage that the carrier may suffer as a result of diligently executing any instruction pursuant to this article, including compensation that the carrier may become liable to pay for loss of or damage to other goods being carried.

3. The carrier is entitled to obtain security from the controlling party for the amount of additional expense, loss or damage that the carrier reasonably expects will arise in connection with the execution of an instruction pursuant to this article. The carrier may refuse to carry out the instructions if no such security is provided.

4. The carrier's liability for loss of or damage to the goods or for delay in delivery resulting from its failure to comply with the instructions of the controlling party in breach of its obligation pursuant to paragraph 1 of this article shall be subject to articles 17 to 23, and the amount of the compensation payable by the carrier shall be subject to articles 59 to 61.

Article 53
Deemed delivery

Goods that are delivered pursuant to an instruction in accordance with article 52, paragraph 1, are deemed to be delivered at the place of destination, and the provisions of chapter 9 relating to such delivery apply to such goods.

Article 54
Variations to the contract of carriage

1. The controlling party is the only person that may agree with the carrier to variations to the contract of carriage other than those referred to in article 50, subparagraphs 1 (*b*) and (*c*).

2. Variations to the contract of carriage, including those referred to in article 50, subparagraphs 1 (*b*) and (*c*), shall be stated in a negotiable transport document or in a non-negotiable transport document that requires surrender,

or incorporated in a negotiable electronic transport record, or, upon the request of the controlling party, shall be stated in a non-negotiable transport document or incorporated in a non-negotiable electronic transport record. If so stated or incorporated, such variations shall be signed in accordance with article 38.

Article 55
Providing additional information, instructions or documents to carrier

1. The controlling party, on request of the carrier or a performing party, shall provide in a timely manner information, instructions or documents relating to the goods not yet provided by the shipper and not otherwise reasonably available to the carrier that the carrier may reasonably need to perform its obligations under the contract of carriage.

2. If the carrier, after reasonable effort, is unable to locate the controlling party or the controlling party is unable to provide adequate information, instructions or documents to the carrier, the shipper shall provide them. If the carrier, after reasonable effort, is unable to locate the shipper, the documentary shipper shall provide such information, instructions or documents.

Article 56
Variation by agreement

The parties to the contract of carriage may vary the effect of articles 50, subparagraphs 1 (*b*) and (*c*), 50, paragraph 2, and 52. The parties may also restrict or exclude the transferability of the right of control referred to in article 51, subparagraph 1 (*b*).

Chapter 11
Transfer of rights

Article 57
When a negotiable transport document or negotiable electronic transport record is issued

1. When a negotiable transport document is issued, the holder may transfer the rights incorporated in the document by transferring it to another person:

(*a*) Duly endorsed either to such other person or in blank, if an order document; or

(*b*) Without endorsement, if: (i) a bearer document or a blank endorsed document; or (ii) a document made out to the order of a named person and the transfer is between the first holder and the named person.

2. When a negotiable electronic transport record is issued, its holder may transfer the rights incorporated in it, whether it be made out to order or to the order of a named person, by transferring the electronic transport record in accordance with the procedures referred to in article 9, paragraph 1.

Article 58
Liability of holder

1. Without prejudice to article 55, a holder that is not the shipper and that does not exercise any right under the contract of carriage does not assume any liability under the contract of carriage solely by reason of being a holder.

2. A holder that is not the shipper and that exercises any right under the contract of carriage assumes any liabilities imposed on it under the contract of carriage to the extent that such liabilities are incorporated in or ascertainable from the negotiable transport document or the negotiable electronic transport record.

3. For the purposes of paragraphs 1 and 2 of this article, a holder that is not the shipper does not exercise any right under the contract of carriage solely because:

(*a*) It agrees with the carrier, pursuant to article 10, to replace a negotiable transport document by a negotiable electronic transport record or to replace a negotiable electronic transport record by a negotiable transport document; or

(*b*) It transfers its rights pursuant to article 57.

Chapter 12
Limits of liability

Article 59
Limits of liability

1. Subject to articles 60 and 61, paragraph 1, the carrier's liability for breaches of its obligations under this Convention is limited to 875 units of account per package or other shipping unit, or 3 units of account per kilogram of the gross weight of the goods that are the subject of the claim or dispute, whichever

amount is the higher, except when the value of the goods has been declared by the shipper and included in the contract particulars, or when a higher amount than the amount of limitation of liability set out in this article has been agreed upon between the carrier and the shipper.

2. When goods are carried in or on a container, pallet or similar article of transport used to consolidate goods, or in or on a vehicle, the packages or shipping units enumerated in the contract particulars as packed in or on such article of transport or vehicle are deemed packages or shipping units. If not so enumerated, the goods in or on such article of transport or vehicle are deemed one shipping unit.

3. The unit of account referred to in this article is the Special Drawing Right as defined by the International Monetary Fund. The amounts referred to in this article are to be converted into the national currency of a State according to the value of such currency at the date of judgement or award or the date agreed upon by the parties. The value of a national currency, in terms of the Special Drawing Right, of a Contracting State that is a member of the International Monetary Fund is to be calculated in accordance with the method of valuation applied by the International Monetary Fund in effect at the date in question for its operations and transactions. The value of a national currency, in terms of the Special Drawing Right, of a Contracting State that is not a member of the International Monetary Fund is to be calculated in a manner to be determined by that State.

Article 60
Limits of liability for loss caused by delay

Subject to article 61, paragraph 2, compensation for loss of or damage to the goods due to delay shall be calculated in accordance with article 22 and liability for economic loss due to delay is limited to an amount equivalent to two and one-half times the freight payable on the goods delayed. The total amount payable pursuant to this article and article 59, paragraph 1, may not exceed the limit that would be established pursuant to article 59, paragraph 1, in respect of the total loss of the goods concerned.

Article 61
Loss of the benefit of limitation of liability

1. Neither the carrier nor any of the persons referred to in article 18 is entitled to the benefit of the limitation of liability as provided in article 59, or as provided in the contract of carriage, if the claimant proves that the loss resulting

from the breach of the carrier's obligation under this Convention was attributable to a personal act or omission of the person claiming a right to limit done with the intent to cause such loss or recklessly and with knowledge that such loss would probably result.

2. Neither the carrier nor any of the persons mentioned in article 18 is entitled to the benefit of the limitation of liability as provided in article 60 if the claimant proves that the delay in delivery resulted from a personal act or omission of the person claiming a right to limit done with the intent to cause the loss due to delay or recklessly and with knowledge that such loss would probably result.

Chapter 13
Time for suit

Article 62
Period of time for suit

1. No judicial or arbitral proceedings in respect of claims or disputes arising from a breach of an obligation under this Convention may be instituted after the expiration of a period of two years.

2. The period referred to in paragraph 1 of this article commences on the day on which the carrier has delivered the goods or, in cases in which no goods have been delivered or only part of the goods have been delivered, on the last day on which the goods should have been delivered. The day on which the period commences is not included in the period.

3. Notwithstanding the expiration of the period set out in paragraph 1 of this article, one party may rely on its claim as a defence or for the purpose of set-off against a claim asserted by the other party.

Article 63
Extension of time for suit

The period provided in article 62 shall not be subject to suspension or interruption, but the person against which a claim is made may at any time during the running of the period extend that period by a declaration to the claimant. This period may be further extended by another declaration or declarations.

Article 64
Action for indemnity

An action for indemnity by a person held liable may be instituted after the expiration of the period provided in article 62 if the indemnity action is instituted within the later of:

(*a*) The time allowed by the applicable law in the jurisdiction where proceedings are instituted; or

(*b*) Ninety days commencing from the day when the person instituting the action for indemnity has either settled the claim or been served with process in the action against itself, whichever is earlier.

Article 65
Actions against the person identified as the carrier

An action against the bareboat charterer or the person identified as the carrier pursuant to article 37, paragraph 2, may be instituted after the expiration of the period provided in article 62 if the action is instituted within the later of:

(*a*) The time allowed by the applicable law in the jurisdiction where proceedings are instituted; or

(*b*) Ninety days commencing from the day when the carrier has been identified, or the registered owner or bareboat charterer has rebutted the presumption that it is the carrier, pursuant to article 37, paragraph 2.

Chapter 14
Jurisdiction

Article 66
Actions against the carrier

Unless the contract of carriage contains an exclusive choice of court agreement that complies with article 67 or 72, the plaintiff has the right to institute judicial proceedings under this Convention against the carrier:

(*a*) In a competent court within the jurisdiction of which is situated one of the following places:

(i) The domicile of the carrier;

(ii) The place of receipt agreed in the contract of carriage;

(iii) The place of delivery agreed in the contract of carriage; or

(iv) The port where the goods are initially loaded on a ship or the port where the goods are finally discharged from a ship; or

(*b*) In a competent court or courts designated by an agreement between the shipper and the carrier for the purpose of deciding claims against the carrier that may arise under this Convention.

Article 67
Choice of court agreements

1. The jurisdiction of a court chosen in accordance with article 66, subparagraph (*b*), is exclusive for disputes between the parties to the contract only if the parties so agree and the agreement conferring jurisdiction:

(*a*) Is contained in a volume contract that clearly states the names and addresses of the parties and either (i) is individually negotiated or (ii) contains a prominent statement that there is an exclusive choice of court agreement and specifies the sections of the volume contract containing that agreement; and

(*b*) Clearly designates the courts of one Contracting State or one or more specific courts of one Contracting State.

2. A person that is not a party to the volume contract is bound by an exclusive choice of court agreement concluded in accordance with paragraph 1 of this article only if:

(*a*) The court is in one of the places designated in article 66, subparagraph (*a*);

(*b*) That agreement is contained in the transport document or electronic transport record;

(*c*) That person is given timely and adequate notice of the court where the action shall be brought and that the jurisdiction of that court is exclusive; and

(*d*) The law of the court seized recognizes that that person may be bound by the exclusive choice of court agreement.

Article 68
Actions against the maritime performing party

The plaintiff has the right to institute judicial proceedings under this Convention against the maritime performing party in a competent court within the jurisdiction of which is situated one of the following places:

(*a*) The domicile of the maritime performing party; or

(*b*) The port where the goods are received by the maritime performing party, the port where the goods are delivered by the maritime performing party or the port in which the maritime performing party performs its activities with respect to the goods.

Article 69
No additional bases of jurisdiction

Subject to articles 71 and 72, no judicial proceedings under this Convention against the carrier or a maritime performing party may be instituted in a court not designated pursuant to article 66 or 68.

Article 70
Arrest and provisional or protective measures

Nothing in this Convention affects jurisdiction with regard to provisional or protective measures, including arrest. A court in a State in which a provisional or protective measure was taken does not have jurisdiction to determine the case upon its merits unless:

(*a*) The requirements of this chapter are fulfilled; or

(*b*) An international convention that applies in that State so provides.

Article 71
Consolidation and removal of actions

1. Except when there is an exclusive choice of court agreement that is binding pursuant to article 67 or 72, if a single action is brought against both the carrier and the maritime performing party arising out of a single occurrence, the action may be instituted only in a court designated pursuant to both article 66 and article 68. If there is no such court, such action may be instituted in a court designated pursuant to article 68, subparagraph (*b*), if there is such a court.

2. Except when there is an exclusive choice of court agreement that is binding pursuant to article 67 or 72, a carrier or a maritime performing party that institutes an action seeking a declaration of non-liability or any other action that would deprive a person of its right to select the forum pursuant to article 66 or 68 shall, at the request of the defendant, withdraw that action once the defendant has chosen a court designated pursuant to article 66 or 68, whichever is applicable, where the action may be recommenced.

Article 72
Agreement after a dispute has arisen and jurisdiction when the defendant has entered an appearance

1. After a dispute has arisen, the parties to the dispute may agree to resolve it in any competent court.

2. A competent court before which a defendant appears, without contesting jurisdiction in accordance with the rules of that court, has jurisdiction.

Article 73
Recognition and enforcement

1. A decision made in one Contracting State by a court having jurisdiction under this Convention shall be recognized and enforced in another Contracting State in accordance with the law of such latter Contracting State when both States have made a declaration in accordance with article 74.

2. A court may refuse recognition and enforcement based on the grounds for the refusal of recognition and enforcement available pursuant to its law.

3. This chapter shall not affect the application of the rules of a regional economic integration organization that is a party to this Convention, as concerns the recognition or enforcement of judgements as between member States of the regional economic integration organization, whether adopted before or after this Convention.

Article 74
Application of chapter 14

The provisions of this chapter shall bind only Contracting States that declare in accordance with article 91 that they will be bound by them.

Chapter 15
Arbitration

Article 75
Arbitration agreements

1. Subject to this chapter, parties may agree that any dispute that may arise relating to the carriage of goods under this Convention shall be referred to arbitration.

2. The arbitration proceedings shall, at the option of the person asserting a claim against the carrier, take place at:

(*a*) Any place designated for that purpose in the arbitration agreement; or

(*b*) Any other place situated in a State where any of the following places is located:

(i) The domicile of the carrier;

(ii) The place of receipt agreed in the contract of carriage;

(iii) The place of delivery agreed in the contract of carriage; or

(iv) The port where the goods are initially loaded on a ship or the port where the goods are finally discharged from a ship.

3. The designation of the place of arbitration in the agreement is binding for disputes between the parties to the agreement if the agreement is contained in a volume contract that clearly states the names and addresses of the parties and either:

(*a*) Is individually negotiated; or

(*b*) Contains a prominent statement that there is an arbitration agreement and specifies the sections of the volume contract containing the arbitration agreement.

4. When an arbitration agreement has been concluded in accordance with paragraph 3 of this article, a person that is not a party to the volume contract is bound by the designation of the place of arbitration in that agreement only if:

(*a*) The place of arbitration designated in the agreement is situated in one of the places referred to in subparagraph 2 (*b*) of this article;

(*b*) The agreement is contained in the transport document or electronic transport record;

(*c*) The person to be bound is given timely and adequate notice of the place of arbitration; and

(*d*) Applicable law permits that person to be bound by the arbitration agreement.

5. The provisions of paragraphs 1, 2, 3 and 4 of this article are deemed to be part of every arbitration clause or agreement, and any term of such clause or agreement to the extent that it is inconsistent therewith is void.

Article 76
Arbitration agreement in non-liner transportation

1. Nothing in this Convention affects the enforceability of an arbitration agreement in a contract of carriage in non-liner transportation to which this Convention or the provisions of this Convention apply by reason of:

(*a*) The application of article 7; or

(*b*) The parties' voluntary incorporation of this Convention in a contract of carriage that would not otherwise be subject to this Convention.

2. Notwithstanding paragraph 1 of this article, an arbitration agreement in a transport document or electronic transport record to which this Convention applies by reason of the application of article 7 is subject to this chapter unless such a transport document or electronic transport record:

(*a*) Identifies the parties to and the date of the charter party or other contract excluded from the application of this Convention by reason of the application of article 6; and

(*b*) Incorporates by specific reference the clause in the charter party or other contract that contains the terms of the arbitration agreement.

Article 77
Agreement to arbitrate after a dispute has arisen

Notwithstanding the provisions of this chapter and chapter 14, after a dispute has arisen the parties to the dispute may agree to resolve it by arbitration in any place.

Article 78
Application of chapter 15

The provisions of this chapter shall bind only Contracting States that declare in accordance with article 91 that they will be bound by them.

Chapter 16
Validity of contractual terms

Article 79
General provisions

1. Unless otherwise provided in this Convention, any term in a contract of carriage is void to the extent that it:

(*a*) Directly or indirectly excludes or limits the obligations of the carrier or a maritime performing party under this Convention;

(*b*) Directly or indirectly excludes or limits the liability of the carrier or a maritime performing party for breach of an obligation under this Convention; or

(*c*) Assigns a benefit of insurance of the goods in favour of the carrier or a person referred to in article 18.

2. Unless otherwise provided in this Convention, any term in a contract of carriage is void to the extent that it:

(*a*) Directly or indirectly excludes, limits or increases the obligations under this Convention of the shipper, consignee, controlling party, holder or documentary shipper; or

(*b*) Directly or indirectly excludes, limits or increases the liability of the shipper, consignee, controlling party, holder or documentary shipper for breach of any of its obligations under this Convention.

Article 80
Special rules for volume contracts

1. Notwithstanding article 79, as between the carrier and the shipper, a volume contract to which this Convention applies may provide for greater or lesser rights, obligations and liabilities than those imposed by this Convention.

2. A derogation pursuant to paragraph 1 of this article is binding only when:

(*a*) The volume contract contains a prominent statement that it derogates from this Convention;

(*b*) The volume contract is (i) individually negotiated or (ii) prominently specifies the sections of the volume contract containing the derogations;

(*c*) The shipper is given an opportunity and notice of the opportunity to conclude a contract of carriage on terms and conditions that comply with this Convention without any derogation under this article; and

(*d*) The derogation is neither (i) incorporated by reference from another document nor (ii) included in a contract of adhesion that is not subject to negotiation.

3. A carrier's public schedule of prices and services, transport document, electronic transport record or similar document is not a volume contract pursuant to paragraph 1 of this article, but a volume contract may incorporate such documents by reference as terms of the contract.

4. Paragraph 1 of this article does not apply to rights and obligations provided in articles 14, subparagraphs (*a*) and (*b*), 29 and 32 or to liability arising from the breach thereof, nor does it apply to any liability arising from an act or omission referred to in article 61.

5. The terms of the volume contract that derogate from this Convention, if the volume contract satisfies the requirements of paragraph 2 of this article, apply between the carrier and any person other than the shipper provided that:

(*a*) Such person received information that prominently states that the volume contract derogates from this Convention and gave its express consent to be bound by such derogations; and

(*b*) Such consent is not solely set forth in a carrier's public schedule of prices and services, transport document or electronic transport record.

6. The party claiming the benefit of the derogation bears the burden of proof that the conditions for derogation have been fulfilled.

Article 81
Special rules for live animals and certain other goods

Notwithstanding article 79 and without prejudice to article 80, the contract of carriage may exclude or limit the obligations or the liability of both the carrier and a maritime performing party if:

(*a*) The goods are live animals, but any such exclusion or limitation will not be effective if the claimant proves that the loss of or damage to the goods, or delay in delivery, resulted from an act or omission of the carrier or of a person referred to in article 18, done with the intent to cause such loss of or damage to the goods or such loss due to delay or done recklessly and with knowledge that such loss or damage or such loss due to delay would probably result; or

(*b*) The character or condition of the goods or the circumstances and terms and conditions under which the carriage is to be performed are such as reasonably to justify a special agreement, provided that such contract of carriage is not related to ordinary commercial shipments made in the ordinary course of trade and that no negotiable transport document or negotiable electronic transport record is issued for the carriage of the goods.

Chapter 17
Matters not governed by this Convention

Article 82
International conventions governing the carriage of goods by other modes of transport

Nothing in this Convention affects the application of any of the following international conventions in force at the time this Convention enters into force, including any future amendment to such conventions, that regulate the liability of the carrier for loss of or damage to the goods:

(*a*) Any convention governing the carriage of goods by air to the extent that such convention according to its provisions applies to any part of the contract of carriage;

(*b*) Any convention governing the carriage of goods by road to the extent that such convention according to its provisions applies to the carriage of goods that remain loaded on a road cargo vehicle carried on board a ship;

(*c*) Any convention governing the carriage of goods by rail to the extent that such convention according to its provisions applies to carriage of goods by sea as a supplement to the carriage by rail; or

(*d*) Any convention governing the carriage of goods by inland waterways to the extent that such convention according to its provisions applies to a carriage of goods without trans-shipment both by inland waterways and sea.

Article 83
Global limitation of liability

Nothing in this Convention affects the application of any international convention or national law regulating the global limitation of liability of vessel owners.

Article 84
General average

Nothing in this Convention affects the application of terms in the contract of carriage or provisions of national law regarding the adjustment of general average.

Article 85
Passengers and luggage

This Convention does not apply to a contract of carriage for passengers and their luggage.

Article 86
Damage caused by nuclear incident

No liability arises under this Convention for damage caused by a nuclear incident if the operator of a nuclear installation is liable for such damage:

(*a*) Under the Paris Convention on Third Party Liability in the Field of Nuclear Energy of 29 July 1960 as amended by the Additional Protocol of 28 January 1964 and by the Protocols of 16 November 1982 and 12 February 2004, the Vienna Convention on Civil Liability for Nuclear Damage of 21 May 1963 as amended by the Joint Protocol Relating to the Application of the Vienna Convention and the Paris Convention of 21 September 1988 and as amended by the Protocol to Amend the 1963 Vienna Convention on Civil Liability for Nuclear Damage of 12 September 1997, or the Convention on Supplementary Compensation for Nuclear Damage of 12 September 1997, including any amendment to these conventions and any future convention in respect of the liability of the operator of a nuclear installation for damage caused by a nuclear incident; or

(*b*) Under national law applicable to the liability for such damage, provided that such law is in all respects as favourable to persons that may suffer damage as either the Paris or Vienna Conventions or the Convention on Supplementary Compensation for Nuclear Damage.

Chapter 18
Final clauses

Article 87
Depositary

The Secretary-General of the United Nations is hereby designated as the depositary of this Convention.

Article 88
Signature, ratification, acceptance, approval or accession

1. This Convention is open for signature by all States at Rotterdam, the Netherlands, on 23 September 2009, and thereafter at the Headquarters of the United Nations in New York.

2. This Convention is subject to ratification, acceptance or approval by the signatory States.

3. This Convention is open for accession by all States that are not signatory States as from the date it is open for signature.

4. Instruments of ratification, acceptance, approval and accession are to be deposited with the Secretary-General of the United Nations.

Article 89
Denunciation of other conventions

1. A State that ratifies, accepts, approves or accedes to this Convention and is a party to the International Convention for the Unification of certain Rules of Law relating to Bills of Lading signed at Brussels on 25 August 1924, to the Protocol to amend the International Convention for the Unification of certain Rules of Law relating to Bills of Lading, signed at Brussels on 23 February 1968, or to the Protocol to amend the International Convention for the Unification of certain Rules of Law relating to Bills of Lading as Modified by the Amending Protocol of 23 February 1968, signed at Brussels on 21 December 1979, shall at the same time denounce that Convention and the protocol or protocols thereto to which it is a party by notifying the Government of Belgium to that effect, with a declaration that the denunciation is to take effect as from the date when this Convention enters into force in respect of that State.

2. A State that ratifies, accepts, approves or accedes to this Convention and is a party to the United Nations Convention on the Carriage of Goods by Sea concluded at Hamburg on 31 March 1978 shall at the same time denounce that Convention by notifying the Secretary-General of the United Nations to that effect, with a declaration that the denunciation is to take effect as from the date when this Convention enters into force in respect of that State.

3. For the purposes of this article, ratifications, acceptances, approvals and accessions in respect of this Convention by States parties to the instruments listed in paragraphs 1 and 2 of this article that are notified to the depositary after this Convention has entered into force are not effective until such denunciations as may be required on the part of those States in respect of these instruments have become effective. The depositary of this Convention shall consult with the Government of Belgium, as the depositary of the instruments referred to in paragraph 1 of this article, so as to ensure necessary coordination in this respect.

Article 90
Reservations

No reservation is permitted to this Convention.

Article 91
Procedure and effect of declarations

1. The declarations permitted by articles 74 and 78 may be made at any time. The initial declarations permitted by article 92, paragraph 1, and article 93, paragraph 2, shall be made at the time of signature, ratification, acceptance, approval or accession. No other declaration is permitted under this Convention.

2. Declarations made at the time of signature are subject to confirmation upon ratification, acceptance or approval.

3. Declarations and their confirmations are to be in writing and to be formally notified to the depositary.

4. A declaration takes effect simultaneously with the entry into force of this Convention in respect of the State concerned. However, a declaration of which the depositary receives formal notification after such entry into force takes effect on the first day of the month following the expiration of six months after the date of its receipt by the depositary.

5. Any State that makes a declaration under this Convention may withdraw it at any time by a formal notification in writing addressed to the depositary. The withdrawal of a declaration, or its modification where permitted by this Convention, takes effect on the first day of the month following the expiration of six months after the date of the receipt of the notification by the depositary.

Article 92
Effect in domestic territorial units

1. If a Contracting State has two or more territorial units in which different systems of law are applicable in relation to the matters dealt with in this Convention, it may, at the time of signature, ratification, acceptance, approval or accession, declare that this Convention is to extend to all its territorial units or only to one or more of them, and may amend its declaration by submitting another declaration at any time.

2. These declarations are to be notified to the depositary and are to state expressly the territorial units to which the Convention extends.

3. When a Contracting State has declared pursuant to this article that this Convention extends to one or more but not all of its territorial units, a place located in a territorial unit to which this Convention does not extend is not considered to be in a Contracting State for the purposes of this Convention.

4. If a Contracting State makes no declaration pursuant to paragraph 1 of this article, the Convention is to extend to all territorial units of that State.

Article 93
Participation by regional economic integration organizations

1. A regional economic integration organization that is constituted by sovereign States and has competence over certain matters governed by this Convention may similarly sign, ratify, accept, approve or accede to this Convention. The regional economic integration organization shall in that case have the rights and obligations of a Contracting State, to the extent that that organization has competence over matters governed by this Convention. When the number of Contracting States is relevant in this Convention, the regional economic integration organization does not count as a Contracting State in addition to its member States which are Contracting States.

2. The regional economic integration organization shall, at the time of signature, ratification, acceptance, approval or accession, make a declaration to the depositary specifying the matters governed by this Convention in respect of which competence has been transferred to that organization by its member States. The regional economic integration organization shall promptly notify the depositary of any changes to the distribution of competence, including new transfers of competence, specified in the declaration pursuant to this paragraph.

3. Any reference to a "Contracting State" or "Contracting States" in this Convention applies equally to a regional economic integration organization when the context so requires.

Article 94
Entry into force

1. This Convention enters into force on the first day of the month following the expiration of one year after the date of deposit of the twentieth instrument of ratification, acceptance, approval or accession.

2. For each State that becomes a Contracting State to this Convention after the date of the deposit of the twentieth instrument of ratification, acceptance,

approval or accession, this Convention enters into force on the first day of the month following the expiration of one year after the deposit of the appropriate instrument on behalf of that State.

3. Each Contracting State shall apply this Convention to contracts of carriage concluded on or after the date of the entry into force of this Convention in respect of that State.

Article 95
Revision and amendment

1. At the request of not less than one third of the Contracting States to this Convention, the Secretary-General of the United Nations shall convene a conference of the Contracting States for revising or amending it.

2. Any instrument of ratification, acceptance, approval or accession deposited after the entry into force of an amendment to this Convention is deemed to apply to the Convention as amended.

Article 96
Denunciation of this Convention

1. A Contracting State may denounce this Convention at any time by means of a notification in writing addressed to the depositary.

2. The denunciation takes effect on the first day of the month following the expiration of one year after the notification is received by the depositary. If a longer period is specified in the notification, the denunciation takes effect upon the expiration of such longer period after the notification is received by the depositary.

DONE at New York, this eleventh day of December two thousand and eight, in a single original, of which the Arabic, Chinese, English, French, Russian and Spanish texts are equally authentic.

IN WITNESS WHEREOF the undersigned plenipotentiaries, being duly authorized by their respective Governments, have signed this Convention.

Notes

1 The business and legal landscape of electronic commercial transactions

1 [1971] 2 QB 163, at 169.
2 The 23rd Statistical Survey Report on the Internet Development in China (July 2005), China Internet Network Information Center (CNNIC), available at http://www.cnnic.cn/uploadfiles/pdf/2009/3/23/153540.pdf (last visited on 29 June 2009).
3 E-Stats, US Census Bureau, US Department of Commerce, 28 May 2009, available at http://www.census.gov/eos/www/2007/2007reportfinal.pdf (last visited on 29 June 2009).
4 BBC News: eBay seeks sellers for expansion, on 24 June 2005 published at http://news.bbc.co.uk/1/hi/business/4619079.stm (last visited on 25 June 2009).
5 Internet World Stats (updated on 31 March 2009).
6 Eurostat: Information society statistics (2009), reported by the Commission Staff Working Document Report on cross-border e-commerce in the EU, Commission of the European Communities, Brussels, 5.3.2009, SEC(2009) 283 final, available at http://ec.europa.eu/consumers/strategy/docs/com_staff_wp2009_en.pdf (last visited on 29 June 2009).
7 Terrett & Monaghan (2000) in Edwards & Waelde (2000), p. 2.
8 European Commission, working paper eEurope, an Information Society for All, available at http://europe.eu.int/comm/information_society/eeurope/objectives/area03_en.htm (last visited on 20 January 2007).
9 Electronic Commerce: Opportunities and Challenges for Government (1997), at 11.
10 A European Initiative in Electronic Commerce, COM (97) 157 at I (7).
11 Commerce: the activities involved in buying and selling things (*Cambridge Advanced Learner's Dictionary*).
12 Trade: the activity of buying and selling, or exchanging, goods and/or services between people or countries (*Cambridge Advanced Learner's Dictionary*).
13 Business: the activity of buying and selling goods and services, or a particular company that does this, or work you do to earn money (*Cambridge Advanced Learner's Dictionary*).
14 Rosner (2004), p. 483. An example of performance against performance can be when one party supplies statistical data in exchange for the results of a market research.
15 A Global Action Plan for Electronic Commerce, Prepared by Business with Recommendations for Governments, ICC, 2nd edition, October 1999, available at http://www.iccwbo.org/policy/ebitt/id2422/index.html (last visited on 29 June 2009).
16 The Organization for Economic Co-operation and Development (OECD) Ministerial Meeting on the Future of the Internet Economy: a Statistic Profile,

June 2008, available at http://www.oecd.org/dataoecd/49/28/40839436.pdf (last visited on 26 June 2009).

17 Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods 2007, UNCITRAL, United Nations, Vienna, 2009, available at http://www.uncitral.org/pdf/english/publications/sales_publications/PromConfEcom_e.pdf (last visited on 29 June 2009).

18 The United Nations Convention on the Use of Electronic Communications in International Contracts, Resolution adopted by the General Assembly on the report of the Sixth Committee (A/60/515), Agenda Idem 79, A/RES/60/21, 9 December 2005.

19 Explanatory Note – United Nations Convention on the Use of Electronic Communications in International Contracts, New York, 2007, available at http://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf (last visited on 18 April 2007), (hereafter Explanatory Note 2007).

20 Available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html (last visited on 7 April 2007).

21 The Model Law on Electronic Signatures of the United Nations Commission on International Trade Law, Resolution adopted by the General Assembly, on the report of the Sixth Committee (A/56/588 and Corr.1), Agenda Item 16, A/RES/56/80, 24 January 2002.

22 Available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html (last visited on 7 April 2007).

23 Moreno (2001).

24 The Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL), Resolution adopted by the General Assembly on the report of the Sixth Committee (A/51/628), Agenda Idem 148, A/RES/51/162, 30 January 2007.

25 Available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html (last visited on 7 April 2007).

26 Article 11 of the UNCITRAL Model Law on Electronic Commerce.

27 Articles 6–8 of the UNCITRAL Model Law on Electronic Commerce.

28 Article 16 of the UNCITRAL Model Law on Electronic Commerce.

29 'What is ICC' at http://www.iccwbo.org/home/menu_what_is_icc.asp (last visited on 9 June 2009).

30 The ICC eTerms 2004, available at http://www.iccwbo.org/policy/law/id3668/index.html (last visited on 28 June 2009).

31 The ICC Guide of eContracting, available at http://www.iccwbo.org/policy/law/id3670/index.html (last visited on 28 June 2009).

32 ICC Global Action Plan for Electronic Business, July 2002, available at http://www.iccwbo.org/home/e_business/word_documents/3rd%20Edition%20Global%20Action%20Plan.pdf (last visited on 29 June 2009).

33 The OECD Guidelines for Consumer Protection in the Context of Electronic Commerce, 9 December 1999, available at http://www.oecd.org/dataoecd/18/13/34023235.pdf (last visited on 19 June 2009).

34 OECD Guidelines for Consumer Protection in the Context of Electronic Commerce, available at http://www.oecd.org/dataoecd/18/13/34023235.pdf (last visited on 29 June 2009).

35 Directive 2000/31/EC of the European Parliament and the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internet Market (Directive on electronic commerce), O.J. 2000 L 178/1.

36 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures, O.J. 2000 L 13/12.

37 Article 1 of the EC Directive on Electronic Commerce.
38 Article 1 of the EC Directive on Electronic Signatures.
39 As of October 2004, 48 states and the District of Columbia had enacted UETA, ULC Bulletin, available at http://www.nccusl.org/nccusl/newsletters/ULC/ULCbull_Oct04_print.pdf (last visited on 18 November 2004).
40 A summary of the UETA, available at http://www.nccusl.org/Update/uniformact_summaries/uniformacts-s-ueta.asp (last visited on 7 September 2007).
41 UCITA and Related Legislation In Your State, last updated in May 2006, available at http://www.ala.org/ala/washoff/woissues/copyrightb/ucita/states.cfm (last visited on 7 September 2007).
42 A summary of the UCITA, available at http://www.nccusl.org/nccusl/ucita/UCITA_Summary.pdf (last visited on 12 June 2007).
43 National Conference of Commissioners on Uniform State Laws – Summary of Uniform Computer Information Transactions Act, available at http://www.nccusl.org/Update/uniformact_summaries/uniformacts-s-ucita.asp (last visited on 12 June 2009).
44 Law of the People's Republic of China on Electronic Signatures (hereafter Chinese Electronic Signatures Law), PRCLEG 3691, 2004, available at http://www.transasialawyers.com/translation/legis_03_e.pdf (last visited on 17 June 2009).
45 Article 1 of the Chinese Electronic Signatures Law.
46 Article 3 of the Chinese Electronic Signatures Law.

2 Technical and legal barriers to online commerce

1 General Usage for International Digitally Ensured Commerce (GUIDEC) Version II, International Chamber of Commerce (ICC), available at www.iccwbo.org (last visited on 1 June 2009).
2 [1971] 1 Lloyd's Rep 439, at 444.
3 Goode (1997), pp. 1–36, 3.
4 *Arnhold Karberg & Co v Blythe Green Jourdain & Co* [1916] 1 KB 495, CA.
5 Incoterms, produced by the International Chamber of Commerce, are a set of delivery terms that may be voluntarily incorporated into international contracts by agreement between the seller and the buyer.
6 Article 1 of the CISG and Article 2(a) of the UN Convention.
7 Article 1 of the CISG.
8 Article 1 of the UN Convention.
9 Articles 8 and 9 of the UN Convention.
10 Electronic Communications under the CISG, CISG-AC Opinion no 1, Electronic Communications under CISG, 15 August 2003, available at http://cisgw3.law.pace.edu/cisg/CISG-AC-op1.html (last visited on 30 June 2009).
11 *Ibid*.
12 Articles 6 and 10(3) of the UN Convention.
13 Article 10 of the UN Convention.
14 Article 15 of the CISG.
15 Article 18(2) of the CISG.
16 Electronic Communications under the CISG, CISG-AC Opinion no 1, Electronic Communications under CISG, 15 August 2003, available at http://cisgw3.law.pace.edu/cisg/CISG-AC-op1.html (last visited on 30 June 2009).
17 *Ibid*.
18 Proposal for a Directive of the European Parliament and of the Council on Consumer Rights, Commission of European Communities, Brussels, 8.10.2008, COM(2008) 614 final, 2008/0196 (COD), available at http://ec.europa.eu/consumers/rights/docs/COMM_PDF_COM_2008_0614_F_EN_PROPOSITION_DE_DIRECTIVE.pdf (last visited on 29 June 2009).

19 Proposal for a Directive on Consumer Rights, EUROPA, Consumer Affairs, available at http://ec.europa.eu/consumers/rights/cons_acquis_en.htm (last visited on 29 June 2009).
20 Recital 10 of the Proposal for a Directive on Consumer Rights.
21 *Leduc v Ward* [1888] 20 QBD 457.
22 Per Salmon J. in *British Imex Industries Ltd v Midland Bank Ltd* [1958] 2 QB 542, at 551.
23 *Sanders Bros v Maclean* (1983) 11 QBD 327.
24 Beecher (2006), pp. 627–48.
25 Girvin (2007), pp. 162–63.
26 UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, United Nations, New York, 1999, available at http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf (last visited on 29 June 2009).
27 The United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea, UNCITRAL, General Assembly, Sixty-third session, A/RES/63/122, available at http://www.uncitral.org/pdf/english/workinggroups/wg_3/CTCRotterdamRulesE.pdf (last visited on 30 June 2009).
28 The Organization for Economic Co-operation and Development (OECD) Ministerial Meeting on the Future of the Internet Economy: a Statistic Profile, June 2008, available at http://www.oecd.org/dataoecd/49/28/40839436.pdf (last visited on 26 June 2009).
29 Articles 4 and 5 of the UCP 600.
30 [1981] 2 WLR 1233.
31 [1966] 1 Lloyd's Rep 367.
32 Article 1(a) of the eUCP V1.1.

Part II Electronic contracts

1 Faria (2006), pp. 689, 691.
2 United Nations Convention on the Use of Electronic Communications in International Contracts, 2005, A/RES/60/21, available at http://daccessdds.un.org/doc/UNDOC/GEN/N05/488/80/PDF/N0548880.pdf?OpenElement (last visited on 10 June 2007).
3 Article 13 of the UN Convention.
4 Article 10(3) of the EC Directive on Electronic Commerce.
5 Explanatory Note 2007, p. 71.
6 Ghoshray (2005), pp. 609, 619.
7 UETA, §14.
8 Explanatory Note 2007, p. 40.
9 Article 12 of the UN Convention.
10 *Ibid.*
11 Explanatory Note 2007, p. 69.
12 Explanatory Note 2007, p. 70.

3 What is an electronic contract?

1 General Usage for International Digitally Ensured Commerce (GUIDEC) Version II, International Chamber of Commerce (ICC), available at www.iccwbo.org (last visited on 1 October 2005).
2 United Nations Convention on the Use of Electronic Communications in International Contracts, 2005, A/RES/60/21, available at http://daccessdds.un.org/doc/UNDOC/GEN/N05/488/80/PDF/N0548880.pdf?OpenElement (last visited on 10 June 2007).
3 Article 4(b) of the UN Convention.

4 Wei & Suling (2006), pp. 116, 136.
5 Article 11 of the UNCITRAL Model Law on Electronic Commerce.
6 Ong (2004), pp. 101, 103.
7 Murray (2000a), pp. 17–35, 19.
8 Campbell & Berenstein (2002), p. 3.
9 §209 of the Uniform Computer Information Transactions Act.
10 Article 9 of the UN Convention.
11 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce), 17.7.2000 *Official Journal of the European Communities* L178/1, Article 9 (Treatment of contracts); Article 10 (Information to be provided); Article 11 (Placing of the order).
12 Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee – First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce), COM/2003/0702 final.
13 Zhang & Lei (2005).
14 Contract Law of People's Republic of China, adopted and promulgated by the second session of the Ninth National People's Congress on 15 March 1999.
15 Article 10 of the Chinese Contract Law states: 'A contract may be made in a writing, in an oral conversation, as well as in any other form'.
16 Article 11 of the Chinese Contract Law.
17 Article 1(1) of the UN Convention.
18 Article 1(2) of the UN Convention.
19 Explanatory Note 2007, p. 51.
20 Explanatory Note 2007, p. 51.
21 Explanatory Note 2007, p. 53.
22 A/CN.9/527, Report of the Working Group IV (Electronic Commerce) on the work of its fortieth session (Vienna 14–18 October 2002), para.108 (hereafter A/CN.9/527).
23 Leng (2006), pp. 234, 237.
24 A/CN.9/527, para.108.
25 §2 and §14 of the Uniform Electronic Transactions Act.
26 Articles 30 and 31 of the China Electronic Signatures Law.
27 Article 6(b) of the EC Directive on Electronic Commerce.

4 When is an electronic contract made?

1 Report of the Working Group on Electronic Commerce on the Work of its 42nd session (Vienna, 17–21 November 2003) (A/CN.9/546), p. 103 (hereafter A/CN.9/546).
2 Explanatory Note 2007, p. 59.
3 Report of the Working Group on Electronic Commerce (A/CN.9/571), p. 142.
4 Wei & Suling (2006), pp. 116, 137.
5 Article 15(1) of the Model Law on Electronic Commerce; §15(a) of the UETA.
6 Explanatory Note 2007, p. 51.
7 *Ibid*.
8 Comments of the UETA from the Annual Conference Meeting in its One-hundred and eighth Year in Denver, Colorado, 23–30 July 1999, p. 53.
9 Article 10(2) of the UN Convention.
10 *Ibid*.

11 Article 15(b)(2) of the UETA.
12 Explanatory Note 2007, p. 63.
13 Ramberg (2001), p. 3. 'Electronic record' means a record created, generated, sent, communicated, received, or stored by electronic means under §2(7) of the UETA, whereas, 'electronic communication' means any communication that the parties make by means of data messages under Article 4(b) of the UN Convention.
14 'Data message' means information generated, sent, received or stored by electronic, magnetic, optical or similar means, including, but not limited to, electronic data interchange, electronic mail, telegram, telex or telecopy.
15 The section of offer and acceptance is an update and reprint of the author's journal article: Wang (2008b), pp. 271–78.
16 Electronic Communications under the CISG, CISG-AC Opinion no 1, Electronic Communications under CISG, 15 August 2003, available at http://cisgw3.law.pace.edu/cisg/CISG-AC-op1.html (last visited on 30 June 2009).
17 Electronic Communications under the CISG, CISG-AC Opinion no 1, Electronic Communications under CISG, 15 August 2003, available at http://cisgw3.law.pace.edu/cisg/CISG-AC-op1.html (last visited on 30 June 2009).
18 [1955] 2 QB 327; [1955] 2 All ER 493.
19 Stone (2005), p. 52.
20 [1983] 2 AC 34.
21 Stone (2005), p. 55.
22 Savirimuthu (2005), pp. 105, 115.
23 Gringras (2003), p. 24.
24 Article 11 of the UN Convention on the Use of Electronic Communications in International Contracts.
25 [1953] 1 QB 401 (CA).
26 Explanatory Note 2007, p. 66.
27 Article 11 of the UN Convention.
28 Explanatory Note 2007, p. 67.
29 *Ibid*, p. 68.
30 [1896] AC 325 (HL).
31 [1976] 1 WLR 1 (HL).
32 Article 11(1)(a) of the EC Directive on Electronic Commerce.
33 *Ibid*, Article 11(3).
34 UCITA §202(a) (2001), available at http://www.law.upenn.edu/bll/ulc/ucita/ucita200.htm (last visited on 2 January 2007).
35 *Ibid*, §203(4) (2001).
36 Watnick (2004), pp. 175, 197.
37 ESIGN sec 101(h).
38 Mckay (2000).
39 UCITA, §201(a)(1).
40 UCITA, §102 (a)(55); UETA, §2(13).
41 Article 13 of the Chinese Contract Law.
42 Article 23 of the Chinese Contract Law.
43 Chen (2001).
44 *Adams v Lindsell* [1818] 1 B & Ald 681; 106 ER 250.
45 Stone (2005), p. 49.
46 *Adams v Lindsell* [1818] 1 B & Ald 681; 106 ER 250.
47 [1879] 4 Ex D 216.
48 Stone (2005), p. 50.
49 *Ibid*, p. 48.
50 Gardner (1992).
51 Lloyd (2000), p. 242.
52 Stuckey (2005), §1.02.

53 Ong (2004), p. 101.
54 *Holwell Securities Ltd v Hughes* [1974] 1 WLR 155 at 161.
55 Restatement (Second) of Contracts, §64 (1979), cited from Stuckey (2005), §1.02.
56 Ong (2004), p. 101.
57 Article 10 of the UN Convention. It provides that 'the time of receipt of an electronic communication is the time when it becomes capable of being retrieved by the addressee at an electronic address designated by the addressee'.
58 Maxeiner (2003), pp. 109, 114.
59 Explanatory Note 2007, p. 71.
60 Wei & Suling (2006), pp. 116, 126–27.
61 Explanatory Note 2007, p. 71.
62 *Ibid*, p. 72.
63 *Ibid*, pp. 71–72.
64 'Legal Study on Unfair Commercial Practices within B2B e-markets – Final Report', European Commission Study ENTR/04/69, (May 2006), pp. 73–74.
65 *Sweeny v Mulcahy* [1993] ILRM 289.
66 *The Great Peace Shipping Ltd v Tsavliris Salvage (International) Ltd* [2002] 3 WLR 1617.
67 [2008] EWHC 157.
68 Savirimuthu (2005), pp. 105, 126.
69 Explanatory Note 2007, p. 74.
70 Article 14 of the UN Convention.
71 Article 10 of the EC Directive on Electronic Commerce.
72 *Ibid*.
73 Contract Law of the People's Republic of China, 1999, available at http://www.law-bridge.net/english/LAW/20064/0222320014345.html (last visited on 30 June 2009).
74 Time to get real about the net, BBC, 21 March 2003, available at http://news.bbc.co.uk/1/hi/technology/2872429.stm (last visited on 30 June 2009).
75 Ramberg (2001), p. 20.
76 Article 14 of the UN Convention.
77 A/CN.9/546, pp. 102–103.
78 Wei & Suling (2006), pp. 116, 162.
79 Explanatory Note 2007, p. 77 (Sales No.E.07.V.2).
80 Microsoft Outlook 'Recall or replace a message you've already sent', available at http://office.microsoft.com/en-us/outlook/HP052421841033.aspx?pid=CH062556091033 (last visited on 30 March 2009).
81 *Ibid.*
82 [1982] 1 All ER 293.
83 Wei & Suling (2006), pp. 116, 162–63.
84 *Ibid*, p. 163.
85 A/CN.9/546, pp. 188–90.
86 Gringras (2003), p. 28.
87 PECL Report (2005), p. 4.
88 *Ibid*, p. 2.
89 Ecommerce Report (2005), p. 8.
90 *Ibid*, p. 9.
91 *Ibid*, p. 17.

5 Where is the contract made?

1 Gringras (2003), p. 16.
2 Murray (2000a), pp. 17–35.
3 Lloyd (2000), p. 243.

4 Article 4(a) of the UNCITRAL Model Law on Electronic Commerce.
5 *Ibid*, Article 4(b).
6 Article 4(h) of the UN Convention.
7 *Ibid*, Article 6(1).
8 *Ibid*, Article 6(2).
9 *Ibid*, Article 6(4) and (5).
10 §109(d) of the UCITA.
11 Article 4(2) of the Council Regulation (EC) No 593/2008 of the European Parliament and of Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), O.J. L 177/6–16, 4.7.2008, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:177:0006:0016:EN:PDF (last visited on 30 June 2009).
12 Article 5(1)(b) of the Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, O.J. L12/1–22, 16.1.2001, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:012:0001:0023:EN:PDF (last visited on 30 June 2009).

6 Contemporary issue: electronic battle of forms

1 Bartell (2000), p. 208.
2 Maxeiner (2003), pp. 109, 110.
3 'Boilerplate' means general conditions, whilst 'front-form' refers to essential or important conditions.
4 Maxeiner (2003), pp. 109, 111.
5 Stone (2005), p. 41.
6 Forte (2006), p. 98.
7 [1979] 1 WLR 401.
8 *Ibid*, pp. 404–405.
9 Forte (2006), pp. 98, 101.
10 *Ibid*, p. 102.
11 Stemp (2005), pp. 243, 244.
12 Forte (2006), pp. 98, 102.
13 United Nations Convention on Contracts for the International Sale of Goods (CISG), U.N. Doc. A/COF. 97/18 (11 April 1980), available at http://www.uncitral.org (last visited on 28 September 2007).
Article 19 of CISG states: 'A reply to an offer which purports to be an acceptance but contains additions, limitations or other modifications is a rejection of the offer and constitutes a counter-offer.

However, a reply to an offer which purports to be an acceptance but contains additional or different terms which do not materially alter the terms of the offer constitutes an acceptance, unless the offeror, without undue delay, objects orally to the discrepancy or dispatches a notice to that effect. If he does not so object, the terms of the contract are the terms of the offer with the modifications contained in the acceptance.

Additional or different terms relating, among other things, to the price, payment, quality and quantity of the goods, place and time of delivery, extent of one party's liability to the other or the settlement of disputes are considered to alter the terms of the offer materially.'
14 Stemp (2005), pp. 243, 261.
15 *Ibid*.
16 Del Duca (2005–06), pp. 133, 146.
17 UCC §2–207 Additional Terms in Acceptance or Confirmation:

> A definite and seasonable expression of acceptance or a written confirmation which is sent within a reasonable time operates as an acceptance even though it states terms additional to or different from those offered or agreed upon, unless acceptance is expressly made conditional on assent to the additional or different terms.
>
> The additional terms are to be construed as proposals for addition to the contract. Between merchants such terms become part of the contract unless:
>
> > the offer expressly limits acceptance to the terms of the offer;
> > they materially alter it; or
> > notification of objection to them has already been given or is given within a reasonable time after notice of them is received.

Conduct by both parties which recognises the existence of a contract is sufficient to establish a contract for sale although the writings of the parties do not otherwise establish a contract. In such case the terms of the particular contract consist of those terms on which the writings of the parties agree, together with any supplementary terms incorporated under any other provisions of this Act.

18 §2–207(2) of UCC.

19 Available at http://dictionary.cambridge.org (last visited on 2 August 2007).

20 Available at http://www.askoxford.com/dictionaries/?view=uk (last visited on 2 August 2007).

21 Forte (2006), pp. 98, 113.

22 Torre & Allen (2006), pp. 195, 202–209.

23 Murray (2000b), 1, p. 41.

24 UNIDROIT Principles of International Commercial Contracts (1994), 34 I.L.M. 1067 (1995), available at http://www.unidroit.org/english/principles/contracts/principles1994/fulltext.pdf
UNIDROIT Principles of International Commercial Contracts (PICC) Article 2.1.11 states:

> (1) A reply to an offer which purports to be an acceptance but contains additions, limitations or other modifications is a rejection of the offer and constitutes a counter-offer.
> (2) However, a reply to an offer which purports to be an acceptance but contains additional or different terms which do not materially alter the terms of the offer constitutes an acceptance, unless the offeror without due delay, objects to the discrepancy. If the offeror does not object, the terms of the contract are the terms of the offer with the modifications contained in the acceptance.

UNIDROIT PICC Article 2.1.22 furthermore provides: 'Where both parties use standard terms and reach agreement except on those terms, a contract is concluded on the basis of the agreed terms and of any standard terms which are common in substance unless one party clearly indicates in advance, or later and without undue delay informs the other party, that it does not intend to be bound by such a contract.'

25 The Principles of European Contract Law (PECL) Article 2:208 states:

> (1) A reply by the offeree which states or implies additional or different terms which would materially alter the terms of the offer is a rejection and a new offer.
> (2) A reply which gives a definite assent to an offer operates as an acceptance even if it states or implies additional or different terms, provided these do not materially alter the terms of the offer. The additional or different terms then become part of the contract.
> (3) However, such a reply will be treated as a rejection of the offer if:

(a) the offer expressly limits acceptance to the terms of the offer; or
(b) the offeror objects to the additional or different terms without delay; or
(c) the offeree makes its acceptance conditional upon the offeror's assent to the additional or different terms, and the assent does not reach the offeree within a reasonable time.

PECL Article 2:209 provides:

(1) If the parties have reached agreement except that the offer and acceptance refer to conflicting general conditions of contract, a contract is nonetheless formed. The general conditions form part of the contract to the extent that they are common in substances.
(2) However, no contract is formed if one party:

(a) has indicated in advance, explicitly, and not by way of general conditions, that it does not intend to be bound by a contract on the basis of paragraph (1); or (b) without delay, informs the other party that it does not intend to be bound by such contract.

(3) General conditions of contract are terms which have been formulated in advance for an indefinite number of contracts of a certain nature, and which have not been individually negotiated between the parties.

26 Forte (2006), pp. 98, 117.
27 Stemp (2005), pp. 243, 266.
28 Article 40 of the Contract Law of the People's Republic of China.
29 The Contract Law of People's Republic of China, 1999, available at http://www.law-bridge.net/english/LAW/20064/0222320014345.html (last visited on 30 June 2009).
30 Article 30 of the Contract Law of the People's Republic of China.
31 Article 15(1) of the UN Convention.
32 *Ibid*, Article 13.
33 *Ibid*, Article 14.
34 Mootz (2007), pp. 14–18.
35 Stone (2005), p. 53.
36 Kidd, Jr & Daughtrey, Jr (2000), pp. 215, 265. Article 11 of the CISG states that 'a contract of sale need not be concluded in or evidenced by writing and is not subject to any other requirement as to form. It may be proved by any means, including witnesses'. Article 1.2 of the PICC provides that 'Nothing in these Principles requires a contract, statement or any other act to be made in or evidenced by a particular form. It may be proved by any means, including witnesses'. Article 2:101(2) of the PECL provides that 'a contract need not be concluded or evidenced in writing nor is it subject to any other requirement as to form. The contract may be proved by any means, including witnesses'.
37 §216 of the Restatement (second) of Contracts (1981).
38 Ramberg (2001), p. 25.
39 Article 11 of the EC Directive on Electronic Commerce.
40 Ramberg (2001), p. 14.
41 The United Nations Convention on the Use of Electronic Communications in International Contracts, (A/60/515).
42 Pappas (2002).

7 Electronic signatures

1 Julia-Barcelo & Vinje (1998).
2 Gringras (2003), p. 38.

3 Gladstone (1997), pp. 13, 36.
4 'E-Commerce: Safety Guide', by PayPal and eBay, p. 6, available at http://pages.ebay.com/merchantsolutions/PayPal_eBay_eCommerceSafetyGuide.pdf (last visited on 8 May 2007).
5 Lessig (2001), pp. 329, 330–31.
6 Anderson (2005), pp. 1441, 1449.
7 Spyrelli (2002).
8 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures, Off.J.EC L13/12 (19/01/2000), at http://europa.eu.int/comm/dg15/en/media/sign/99-915.htm (last visited on 3 June 2004).
9 Uniform Electronic Transactions Act, available at http://www.nccus/org/uniformact_summaries/uniformacts-s-s-ueta.htm (last visited on 4 June 2004).
10 The US Electronic Signatures in Global and National Commerce Act 2000 (E-Sign Act), available at http://www.ftc.gov/os/2001/06/esign7.htm (last visited on 28 September 2007).
11 Law of the People's Republic of China on Electronic Signature, 28/08/2004, the 11th meeting of the Standing Committee of the Tenth National People's Congress of the People's Republic of China, available at http://www.law-bridge.net/english/LAW/20064/0221374918883.shtml (last visited on 28 September 2007).
12 Available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce.html (last visited on 28 September 2007).
13 *Goodman v J Eban Ltd* [1954] 1 All ER 763.
14 Rubber stamps affixed to a document can establish valid signatures, *Lazarus Estates, Ltd v Beasley* [1956] 1 QB 702.
15 Bharvada (2002).
16 UNCITRAL Model Law on Electronic Signatures (2001) at http://www.uncitral.org (last visited on 2 June 2004).
17 Article 2(1) of the EC Directive on Electronic Signatures.
18 Prefatory Note and Comments on the Uniform Electronic Transactions Act, 1999, available at http://www.law.upenn.edu/bll/archives/ulc/fnact99/1990s/ueta99.htm (last visited on 30 August 2007).
19 §106 (5) of US E-sign Act 2000.
20 Article 2 of the Law of the People's Republic of China on Electronic Signature (Chinese Electronic Signatures Law).
21 Smart card is a plastic card containing a microprocessor (a chip) that can generate, store, and process data, and can be programmed to be activated only when the user enters a PIN or other identifier.
22 Biometrics are technologies for measuring and analysing human body characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements to authenticate their identity.
23 Signature Creator 1.12, available at http://wareseeker.com/screenshot/signature-creator-1.12.exe/259645 (last visited on 30 June 2009).
24 '2007 – Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods', the United Nations Commission on International Trade Law (UNCITRAL), Vienna, United Nations, released in 2009, available at http://www.uncitral.org/pdf/english/publications/sales_publications/PromConfEcom_e.pdf (last visited on 1 June 2009).
25 'ABA's Digital Signature Guidelines' at http://www.abanet.org/ftp/pub/scitech/ds-ms.doc (last visited on 4 July 2004).
26 Basu & Jones (2003).
27 Fresen (1997).
28 Bharvada (2002), pp. 265, 268.
29 Wild, Weinstein & MacEwan (2005), p. 67.

30 Capps (2002).
31 Further explanations and details are available at 'UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001', United Nations, New York, 2002, pp. 39–40, http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf (last visited on 28 September 2007).
32 Angel (1999).
33 Spyrelli (2002).
34 Baker & Yeo (1999).
35 Tosto & Baracks (1996).
36 Anderson (2005), pp. 1441, 1463.
37 UN Convention on the Use of Electronic Communications on International Contracts (The UN Convention), 2005, available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html (last visited on 30 August 2007).
38 Article 7(1)(a) of the UNCITRAL Model Law on Electronic Commerce.
39 Article 9(3)(a) of the UN Convention.
40 UNCITRAL Model Law on Electronic Signatures, Article 6(3)(d); UNCITRAL Model Law on Electronic Commerce, Article 7(1)(a).
41 [2006] EWHC 813 (Ch); [2006] 1 WLR 1543; [2006] 2 All ER 891, 7 April 2006.
42 Section 4 of the Statute of Frauds.
43 [2006] 1 WLR 1543, at 1546, para.10.
44 *Ibid*, at 1548, para.16.
45 *Ibid*, at 1550, para.20.
46 [1892] 1 QB 593.
47 [1892] 1 QB 593, at 597.
48 [2006] 1WLR 1543, at 1552.
49 *Ibid*.
50 'E-commerce: Safety Guide', by PayPal and eBay, available at http://pages.ebay.com/merchantsolutions/PayPal_eBay_eCommerceSafetyGuide.pdf (last visited on 8 May 2007).
51 Report of the Working Group on Electronic Commerce on the work of its 42nd session (Vienna, 17–21 November 2003) (A/CN.9/546), pp. 48, 54–57.
52 Wei & Suling (2006), pp. 116, 130.
53 *Ibid*.
54 EU Commission Legal-IST Project, 'Report on Legal Issues of Software Agents', p. 64.

8 Electronic authentication

1 §102(a)(6) of the UCITA.
2 2007 – Promoting confidence in Electronic Commerce: legal issues on International Use of Electronic Authentication and Signature Method, UNCITRAL, Vienna, United Nations, 2009, available at http://www.uncitral.org/pdf/english/publications/sales_publications/PromConfEcom_e.pdf (last visited on 30 June 2009).
3 *Ibid*.
4 Recktenwald (2004).
5 'Authentication – Digital Signatures Guideline' (1999) 2.1 Office of Information and Communications Technology from Department of Commerce in Australia, at http://www.commerce.nsw.gov.au (last visited on 15 August 2004).
6 United Nations Commission on International Trade Law (UNCITRAL), Fortieth Session, Possible future work on electronic commerce, Comprehensive reference document on elements required to establish a favourable legal framework

for electronic commerce: sample chapter on international use of electronic authentication and signature methods, Vienna, 25 June–12 July 2007, A/CN.9/630, p. 4.

7 *Farm Credit Bank of St Paul v William G Huether*, 12 April 1990 (454 N.W. 2d 710, 713) (United States, Supreme Court of North Dakota, North Western Reporter), cited from A/CN.9/630, p. 5.
8 *Alfred E Weber v Dante De Cecco*, 14 October 1948 (1 N.J. Super. 353, 358) (United States, New Jersey Superior Court Reports), cited from A/CN.9/630, p. 5.
9 Bainbridge (2008), pp. 360–61.
10 'Selected Bibliography on Description of Digital Signatures', Appendix 6 of 'The Role of Certification Authorities in Consumer Transactions', Working Groups and Publications, Internet Law and Policy Forum, available at http://www.ilpf.org/groups/ca/app6.htm (last visited on 27 August 2007), hereafter Description of Digital Signatures.
11 Osty & Pulcanio (Spring 1999).
12 'The Role of Certification Authorities in Consumer Transactions' (Working Groups and Publications, Internet Law and Policy Forum) at http://www.ilpf.org/groups/ca/draft.htm (last visited on 25 June 2004).
13 'UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001', United Nations, New York, 2002, available at http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf (last visited on 28 September 2007), p. 40.
14 Akdeniz, Clarke, Kelman & Oram (1997).
15 Available at http://www.paypal.com (last visited on 8 May 2007).
16 'E-Commerce: Safety Guide', by PayPal and eBay, available at http://pages.ebay.com/merchantsolutions/PayPal_eBay_eCommerceSafetyGuide.pdf (last visited on 8 May 2007).
17 Smedinghoff (1996).
18 Hindelang (2002).
19 Osty & Pulcanio (1999), pp. 961, 966.
20 Description of Digital Signatures.
21 Wu (2000).
22 'United States Postal Service Certification Practice Statement', the United States Postal Service, Version 1, Handbook AS-600, February 2001, available at http://www.apwu.org/dept/ind-rel/USPS_hbks/AS-Series/AS-600%20USPS%20Certification%20Practice%20Statement%202-01%20(170% 20KB).pdf (last visited on 30 August 2007).
23 Available at www.verisign.com (last visited on 30 August 2007).
24 Baker & Yeo (1999).
25 Wu (2000), pp. 9–10.
26 Article 46–3–201 of the Utah Digital Signature Act.
27 Lloyd (2004), p. 662.
28 Section 3.11 of the ABA Draft Guidelines.
29 Froomkin (1996).
30 *Ibid*.
31 'Building Confidence in Electronic Commerce', A Consultation Document, URN 99/642, Department of Trade and Industry, available at http://www.cyber-rights.org/crypto/consfn1.pdf (last visited on 27 August 2007).
32 Hindelang (2002), p. 10.
33 Recital 22 of the EC Directive on Electronic Signatures.
34 Froomkin (1996).
35 Unless they have reason to know of the errors, publishers and book distributors are not liable for errors in works they publish and sell. See, e.g., *ALM v Van Nostrand Reinhold Co*, 480 N.E.2d 1263 (Ill. App. 1985) (dismissing negligence claim against publisher of allegedly unsafe How To book); *Cardozo v True*, 342

So. 2d 1053 (Fla. Dist. Ct. App.) (holding UCC did not make book dealer liable to purchaser of cookbook for lack of adequate warnings as to poisonous ingredients used in recipe), cert. denied, 353 So. 2d 674 (Fla. 1977).
36 Guest (1989).
37 Hindelang (2002), p. 16.
38 'Report on CA Responsibilities and Liability for Cross-Border E-Commerce', 31 July 2005, Legal Infrastructure Working Group, Asia PKI Forum, available at http://www.japanpkiforum.jp/shiryou/APKI-F/CA_Responsibility_20050830.pdf (last visited on 27 August 2007).
39 Recital (40) of the EC Directive on Electronic Commerce.
40 Article 11 of the UNCITRAL Model Law on Electronic Signatures.
41 Article 6 of the EC Directive on Electronic Signatures.
42 Osty & Pulcanio (1999).
43 *Ibid*.
44 'The Role of Certification Authorities in Consumer Transactions' (Working Groups and Publications, Internet Law and Policy Forum) at http://www.ilpf.org/groups/ca/draft.htm (last visited on 25 June 2004).
45 Article 6(3) of the EC Directive on Electronic Signatures.
46 *Ibid*, Article 6(4).
47 Froomkin (1996).
48 EC Directive on Electronic Signatures.
49 *Ibid*.
50 *Ibid*.
51 Article 7 of the EC Directive on Electronic Signatures.
52 Blythe (2005), p. 6, para.49.
53 Boss (1998), pp. 1931, 1963.
54 Spyrelli (2002).
55 Diedrich (2000).
56 §101(a) of E-Sign Act 2000.
57 *Ibid*.
58 Blythe (2005), p. 6, para.50.
59 'European Commission Approves Network for E-Signature Authentication', available at http://www.devicelink.com/emdm/archive/01/01/013e.htm (last visited on 2 June 2004).
60 Article 1 of the Chinese Electronic Signatures Law.
61 Carnabuci & Li (2005), N69.
62 Chan (2005), pp. 47–50, 48.
63 Articles 4 and 9 of the Chinese Electronic Signatures Law.
64 Articles 16–19 of the Chinese Electronic Signatures Law.
65 Carnabuci & Li (2005), p. 69.
66 Chan (2005), pp. 47–50, 49.
67 'UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001', United Nations, New York, 2002, available at http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf (last visited on 28 September 2007), p. 42.
68 Murray (2003).
69 Article 12(5) of the Model Law on Electronic Signatures.
70 Craig (2004).
71 Spyrelli (2002).
72 A/CN.9/630, p. 1.
73 '2007 – Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods', the United Nations Commission on International Trade Law (UNCITRAL), Vienna, United Nations, released in 2009, available at http://www.uncitral.org/pdf/english/publications/sales_publications/PromConfEcom_e.pdf (last visited on 1 June 2009).

74 *Ibid.*
75 OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication (Paris, June 2007), available at http://www.oecd.org/dataoecd/32/45/38921342.pdf (last visited on 30 June 2009).
76 '2007 – Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods', the United Nations Commission on International Trade Law (UNCITRAL), Vienna, United Nations, released in 2009, available at http://www.uncitral.org/pdf/english/publications/sales_publications/PromConfEcom_e.pdf (last visited on 1 June 2009).

9 Contemporary issue: protecting information in electronic communications

1 'Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods', the United Nations Commission on International Trade Law (UNCITRAL), available at http://www.uncitral.org/pdf/english/publications/sales_publications/PromConfE-com_e.pdf (last visited on 1 June 2009).
2 Mann & Winn (2005), p. 193.
3 Microsoft Windows Product Activation privacy statement, available at http://technet.microsoft.com/en-us/library/cc756122.aspx (last visited on 10 June 2009).
4 Wacks (2001), pp. 75–97, 80.
5 Mann & Winn (2005), p. 194.
6 Part 2: Security, confidentiality, traffic and location data, itemised billing, CLI and directories, Guidance on the Privacy and Electronic Communications (EC Directive) Regulations 2003, Version 3.4, 30 November 2006, Information Commissioner's Office, available at http://www.ico.gov.uk/upload/documents/library/privacy_and_electronic/detailed_specialist_guides/pecr_guidance_part2_1206.pdf (last visited on 10 June 2009).
7 .eu Domain Name WHOIS Policy, v.1.0.2., available at http://www.eurid.eu/files/whois_en.pdf (last visited on 11 June 2009). Further information can be found at http://www.eurid.eu/en/content/whois-result (last visited on 11 June 2009).
8 Firms breaching data protection, BBC News, Wednesday, 11 July 2007, available at http://news.bbc.co.uk/1/hi/business/6289410.stm (last visited on 11 June 2009).
9 Convention for the Protection of Human Rights and Fundamental Freedoms, Council of Europe, Rome, 1950.
10 Ryssdal (1991).
11 27 member states of the EU: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and United Kingdom, available at http://europa.eu/abc/european_countries/index_en.htm (last visited on 12 June 2009).
12 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereafter EC Directive on Data Protection), Official Journal L 281, 23/11/1995 P. 0031–0050.
13 Kuner (2003), p. 79.
14 Article 2(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data.
15 UK Data Protection Act 1998, c.29.
16 Robinson, Graux, Botterman & Valeri (2009).
17 [2003] EWCA Civ 1746.
18 The *Durant* case and its impact on the interpretation of the Data Protection Act

1998, Information Commissioner's Office, 27 February 2006, available at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/the_durant_case_and_its_impact_on_the_interpretation_of_the_data_protection_act.pdf (last visited on 12 June 2009).

19 *Durant v the Financial Services Authority (FSA)* [2003] EWCA Civ 1746.

20 Press Release: New guidance 'Durant v Financial Services Authority Court of Appeal's ruling', Information Commissioner, 3 February 2004, available at http://www.ico.gov.uk/upload/documents/pressreleases/2004/pr%20new%20guidance%20-%20durant%20v%20fsa.pdf (last visited on 9 June 2009).

21 Article 7(a) and (b) of the EC Directive on Data Protection.

22 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215, 25.8.2000, pp. 7–47.

23 'Safe Harbour Overview', US Department of Commerce, available at http://www.export.gov/safeharbor/eg_main_018236.asp (last visited on 6 June 2009).

24 Measures for Security Protection Administration of the International Networking of Computer Information Networks, The Ministry of Public Security of the People's Republic of China, No. 33, available at http://www.mps.gov.cn/n16/n1282/n3493/n3823/n442104/452202.html (last visited on 9 June 2009).

25 Regulation of the People's Republic of China for Security Protection of Computer Information System, the State Council of the People's Republic of China, Decree No. 147, 1994, available at http://www.en8848.com.cn/yingyu/84/n-92584.html (last visited on 9 June 2009).

26 Hangzhou Measures for Computer Information Network Security Protection Administration, the Standing Committee of the People's Congress in Hangzhou City, Zhejiang Province, No. 17, available at http://www.chinacourt.org/flwk/show.php?file_id=135270 (last visited on 9 June 2009).

27 The Regulation of the Guangdong Provision for Security Protection of Computer Information System, Standing Committee of the People's Congress in Guangzhou Province, http://www.gdemo.gov.cn/ywwk/fgk/gdsflfg/shaqlfg/shaqsjlgdsfggz/200801/t20080107_39165.htm (last visited on 9 June 2009).

28 China to legislate for protection of personal information, by People's Daily Online, 25 January 2005, available at http://english.peopledaily.com.cn/200501/25/eng20050125_171801.html (last visited on 9 June 2009).

29 About APEC, http://www.apec.org/apec/about_apec.html (last visited on 13 June 2009).

30 Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Paris, 1980), available at http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (last visited on 12 June 2009).

31 Implementing the OECD 'Privacy Guidelines' in Electronic Environment: Focus on the Internet, Group of Experts on Information Security and Privacy, DSTI/ICCP/REG(97)6/FINAL, 09 September 1998, available at http://www.oecd.org/dataoecd/33/43/2096272.pdf (last visited on 12 June 2009).

32 OECD 'Report on the Cross-border Enforcement of Privacy Laws', available at http://www.oecd.org/dataoecd/17/43/37558845.pdf (last visited on 12 June 2009).

33 Members of the Asia-Pacific Economic Co-operation (APEC): Australia, Brunei Darussalam, Canada, Chile, China, Hong Kong (China), Indonesia, Japan, Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Russia, Singapore, Chinese Taipei, Thailand, United States and Viet

Nam, available at http://www.apec.org/apec/news___media/fact_sheets/apec_participation.html (last visited on 10 June 2009).

34 APEC Privacy Framework, 16th APEC Ministerial Meeting, Santiago, Chile, 17–18 November 2004, 2004/AMM/014rev1.

35 Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods (hereafter E-confidence Note), UNCITRAL, Vienna, 2009, available at http://www.uncitral.org/pdf/english/publications/sales_publications/PromConfEcom_e.pdf (last visited on 16 June 2009).

36 Paragraph 71 of the E-Confidence Note.

37 Paragraph 76 of the E-Confidence Note.

38 Article 1 of the EC Directive on Data Protection 1995.

39 EDPS second Opinion on ePrivacy Directive review and security breach: privacy safeguards need to be strengthened, Press Release, Brussels, Monday 12 January 2009, available at http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/PressNews/Press/2009/EDPS-2009-01_ePrivacy_2_EN.pdf (last visited on 14 June 2009).

40 Second opinion of the European Data Protection Supervisor on the review of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), O.J. C 128/33, 6.6.2009, available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-01-09_ePricacy_2_EN.pdf (last visited on 12 June 2009).

41 Cooper, Fink, Jones and Quathem (2006).

42 [2008] EWHC 1781 (QB).

43 FTC Public Speech, 1 November 1995, available at http://www.ftc.gov/speeches/varney/varnprvy.shtm (last visited on 16 June 2009).

44 Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress (FTC Fair Information Practices Report), FTC Commission Report, May 2000, available at http://www.ftc.gov/reports/privacy2000/privacy2000text.pdf (last visited on 16 June 2009).

45 Self-Regulation and Privacy Online: A Federal Trade Commission Report to Congress, FTC Commission Report, July 1999, available at http://www.ftc.gov/os/1999/07/privacy99.pdf (last visited on 16 June 2009).

46 Privacy Online: A Report to Congress, FTC Commission Report, June 1998, available at http://www.ftc.gov/reports/privacy3/priv-23a.pdf (last visited on 16 June 2009).

47 FTC Fair Information Practices Report, 2000.

48 The Federal Trade Commission Act (FTCA) and the Children's Online Privacy Protection Act (COPPA).

49 *EPIC v FTC*, Case:1: 08-CV-00448, 14 March 2008.

50 Facebook Executive Discusses Beacon Brouhaha, the New York Times, 29 November 2007, available at http://bits.blogs.nytimes.com/2007/11/29/facebook-responds-to-beacon-brouhaha/ (last visited on 16 June 2009).

51 Opinion 5/2009 on online social networking, by the European Commission Article 29 Data Protection Working Party, WP163, Brussels, 12 June 2009, available at http://epic.org/privacy/socialnet/Opinion_SNS_090316_Adopted.pdf (last visited on 16 June 2009).

52 23rd Statistical Survey Report on the Internet Development in China, by the China Internet Network Information Center (CNNIC), January 2009, available at http://www.cnnic.cn/uploadfiles/pdf/2009/3/23/131303.pdf (last visited on 9 June 2009).

53 Articles 38–40 of the Constitution of the People's Republic of China, Standing Committee of the National People's Congress, 1982, available at http://www.nxycedu.com/Zcfg/Xf/20060913085426.html (last visited on 1 June 2009).

54 Article 101 of the General Principles of the Civil Law of the People's Republic of China, Standing Committee of the National People's Congress of the People's Republic of China, 1986, No 37, available at http://www.englishcn.com/zh/vocations/laws/20070716/4912_9.html (last visited on 1 June 2009).
55 Qin (2008), pp. 234, 249.
56 About Tencent (QQ), available at http://www.tencent.com/en-us/at/abouttencent.shtml (last visited on 1 June 2009).
57 QQ/Tencent Privacy Statement, available at http://www.tencent.com/en-us/le/privacy.shtml (last visited on 9 June 2009).
58 EU–US Safe Harbour Privacy Principles: Notice, Choice, Onward Transfer, Security, Data Integrity, Access and Enforcement.
59 About Alibaba, available at http://news.alibaba.com/specials/aboutalibaba/index.html (last visited on 10 January 2009).
60 Policy Statement of Alibaba.com.cn, available at http://info.china.alibaba.com/biznews/pages/alihome/js_ys.html (last visited on 10 January 2009).
61 Privacy Policy of Alibaba.com, available at http://www.alibaba.com/trade/servlet/page/help/rules_and_policies/privacy_policy (last visited on 10 June 2009).
62 Privacy Online: Policy and Practice Guidance, OECD Working Party on Information Security and Privacy, DSTI/ICCP/REG(2002)3/FINAL, 21 January 2003, available at http://www.olis.oecd.org/olis/2002doc.nsf/LinkTo/NT000029C6/$FILE/JT00137976.PDF (last visited on 16 June 2009).
63 Implementing the OECD 'Privacy Guidelines' in Electronic Environment: Focus on the Internet, Group of Experts on Information Security and Privacy, DSTI/ICCP/REG(97)6/FINAL, 09 September 1998, available at http://www.oecd.org/dataoecd/33/43/2096272.pdf (last visited on 12 June 2009).
64 TRUSTe Watchdog Dispute Resolution and Appeal Process, available at https://www.truste.org/consumers/compliance.php?PHPSESSID=51087adc53dc5bb54875b318ef80b23d; BBBOnline Complaints, available at http://www.bbb.org/us/bbb-faqs/#faq4 (last visited on 16 June 2009).
65 TRUSTe Watchdog Reports, available at https://www.truste.org/consumers/watchdog_reports.php?PHPSESSID=51087adc53dc5bb54875b318ef80b23d (last visited on 19 June 2009).
66 Mann & Winn (2005), p. 227.
67 Swindells & Henderson (1998).

10 Resolving electronic commercial disputes

1 Article 15 of the UNCITRAL Model Law on Electronic Commerce, on the report of the Sixth Committee (A/51/628) 16 DECEMBER 1996, available at www.lexmercatoria.org (last visited on 16 August 2007); and Article 10 of the UN Conventions on the Use of Electronic Communications in International Contracts, 2005, available at www.uncitral.org (last visited on 16 August 2007).
2 Article 6 of the UN Convention on the Use of Electronic Communications in International Contracts.
3 Recital 23 and Article 1(4) of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (hereafter EC Directive on electronic commerce).
4 The EU and US sections of this part is the reprint and update of the author's journal paper: Wang (2008), pp. 233–41.
5 Council Regulation on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters ('Brussels Regulation'), see Council Regulation (EC) No. 44/2001, 22 December 2000, Official Journal L 012,

16.01.2001, p. 1, available at http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_012/l_01220010116en00010023.pdf (last visited on 13 June 2009).

6 Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the application of Council Regulation (EC) No 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, Brussels, 21.4.2009, COM(2009) 174 final, Commission of the European Communities, available at http://www.ipex.eu/ipex/cms/home/Documents/doc_COM20090174FIN (last visited on 18 June 2009).

7 Green Paper on the Review of Council Regulation (EC) No 44/2001 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, Brussels, 21.4. 2009, COM(2009) 175 final, Commission of the European Communities, available at http://www.ipex.eu/ipex/cms/home/Documents/doc_COM20090175FIN (last visited on 18 June 2009).

8 *Lis Pendens:* a pending lawsuit.

9 Morris, McClean & Beevers (2005), p. 87.

10 Convention of 30 June 2005 Choice of Court Agreements (the Hague Convention), the Hague, available at http://www.hcch.net/index_en.php?act=conventions.text&cid=98 (last visited on 18 June 2009).

11 Hague Convention Status Table, available at http://www.hcch.net/index_en.php?act=conventions.status&cid=98 (last visited on 18 June 2009).

12 Article 1(1) of the Hague Convention.

13 *WH Martin Ltd v Feldbinder Spezialfahrzeugwerke GmbH* [1998] ILPr 794.

14 *Castelletti v Trummpy* [1999] ECR I-1597.

15 *Sinochem v Mobil* [2000] 1 Lloyd's Rep 670.

16 *Ibid*.

17 Article 23(2) of Brussels I Regulation.

18 Fawcett, Harris & Bridge (2005), p. 511.

19 Article 2 of Brussels I Regulation.

20 Articles 2 and 59 of Brussels I Regulation.

21 Article 60 of Brussels I Regulation.

22 Fawcett, Harris & Bridge (2005), p. 511.

23 *Ibid*.

24 Article 6 of the UN Convention on the Use of Electronic Communications in International Contracts, A/RES/60/21, 9 December 2005.

25 Article 6(1) of the UN Convention.

26 Article 6(3) of the UN Convention; Article 15(4)(b) of the UNCITRAL Model Law on Electronic Commerce.

27 Article 15(4)(b) of the UNCITRAL Model Law on Electronic Commerce.

28 Article 6(2) of the UN Convention.

29 *Ibid*.

30 Articles 8–14 of the Brussels Regulation govern insurance; Articles 15–17 are about consumer contracts; Articles 18–21 make provisions about employment contracts.

31 Article 5(1) (a) of the Brussels I Regulation states that 'A person domiciled in a Member State may, in another Member Sate, be sued in matters relating to a contract, in the courts for the place of performance of the obligation in question'. 'The obligation in question' means that which is relied upon as the basis for the claim, explained by Morris, McClean & Beevers (2005), p. 72.

32 Hill (2005), p. 135.

33 Case C-420/97 *Leathertex Divisione Sintetici SpA v Bodetex BVBA* [1999] ECR I-6747.

34 Case 266/85 *Shenavai v Kreischer* [1987] ECR 239.

35 *Color Drack GmbH v Lexx International Vertriebs GmbH* (Case C-386/05), [2007] ILPr 35.
36 *Ibid*, at 456.
37 *Ibid*.
38 *Ibid*, at 479.
39 *Ibid*, at 480.
40 *Ibid*, at 473.
41 *Ibid*, at 472.
42 Case C-256/00 *Besix SA v. Wasserreinigungsbau Alfred Kretzschmar GmbH & Co KG (Wabag)* [2002] ECR I-1699.
43 Fawcett, Harris & Bridge (2005), p. 514.
44 Burnett & Klinger (2005), p. 74.
45 Fawcett, Harris & Bridge (2005), p. 1301.
46 Deveci (2006), p. 43.
47 Hague Convention Status Table, available at http://www.hcch.net/index_en.php?act=conventions.status&cid=98 (last visited on 18 June 2009).
48 Chik (2002), pp. 243, 248–49.
49 326 U.S. 310 (1945).
50 Scoles, Hay, Borchers & Symeonides (2000), p. 344.
51 *International Shoe*, 326 U.S. at 320, 66 S.Ct. at 160, 90 L.Ed. at 104.
52 Scoles, Hay, Borchers & Symeonides (2000), p. 348.
53 *Ibid*, p. 338.
54 Restatement, Second, Conflict of Laws §30 (1971).
55 *Helicopteros Nacionales de Colombia, SA v Hall*, 466 U.S. 408 (1984).
56 Scoles, Hay, Borchers & Symeonides (2000), p. 344.
57 *Ashi Metal Ind. Co. v Superior Court*, 480 U.S. 102 (1987).
58 Maloney (1993), pp. 1265, 1269–70.
59 Scoles, Hay, Borchers & Symeonides (2000), p. 300.
60 Smith (2002), p. 347.
61 *Burger King Corp v Rudzewicz*, 471 U.S. 479, 105 S.Ct. 2185, 85 L. Ed. 2d 528 (1985).
62 *World Wide Volkswagen v Woodson*, 444 U.S. 286 (1980).
63 *Ballard v Savage*, 65 F.3d 1495, 1498 (9th Cir. 1995).
64 See *Zippo Mfg. Co. v Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W. D. Pa 1997), at 1124.
65 *Int'l Shoe Co. v State of Wash.*, 326 U.S. 310 (1945).
66 See *Zippo Mfg. Co. v Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W. D. Pa 1997).
67 *Ibid*, at 1124.
68 *CompuServe Inc. v Patterson*, 89 F. 3d. 1267 (6th Cir. 1996).
69 See *Zippo Mfg. Co. v Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W. D. Pa 1997), at 1124; see also *Maritz Inc. v Cybergold Inc.* 947 F Supp 1328 (ED Mo1996).
70 See *Zippo Mfg. Co. v Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W. D. Pa 1997), at 1124.
71 Boone (2006), pp. 241, 258.
72 Rice (2004), p. 11, 52.
73 *Calder v Jones*, 465 U.S. 783 (1984). In Calder, a California resident brought suit in California Superior Court against Florida residents who allegedly wrote libellous matter about her in a prominent national publication. In holding that jurisdiction was proper, the Court found 'the brunt of the harm, in terms both of respondent's emotional distress and the injury to her professional reputation, was suffered in California.'
74 Boone (2006), pp. 241, 260.
75 *Ibid*, pp. 241, 261.
76 Rice & Gladstone (2003), pp. 601, 629.
77 *Cybersell, Inc. v Cybersell, Inc.*, 130 F. 3d 414, 420 (9th Cir. 1997).

78 *Bancroft & Masters, Inc. v Augusta Nat'l Inc.*, 223 F. 3d 1082, 1087 (9th Cir. 2000).
79 *Ibid*.
80 Geist (2001).
81 *Ibid*.
82 *World-Wide Volkswagen Corp. v Woodson*, 444 U.S. 286, 297 (1980).
83 Berman (2002), pp. 311, 418.
84 Aciman & Vo-Verde (2002), pp. 16, 19, and also *ALS Scan, Inc. v Digital Serv. Consultants, Inc.*, 293 F. 3d 707, 714 (4th Cir. 2002).
85 Boone (2006), pp. 241, 266.
86 *Ibid*, pp. 241, 274.
87 Wang (2008), pp. 233–41.
88 Articles 237–270 of the Civil Procedure Law of the People's Republic of China, promulgated on 9 April 1991.
89 Article 24 of the Civil Procedure Law of the People's Republic of China.
90 Article 25 of the Civil Procedure Law of the People's Republic of China, available at http://en.chinacourt.org/public/detail.php?id=2694 (last visited on 27 August 2007).
91 Article 244 of the Civil Procedure Law provides that 'Parties to a dispute over a contract involving foreign interests or over property rights and interests involving foreign interests may, through written agreement, choose the people's court in the place which has actual connections with the dispute as the jurisdictional court. If a people's court of the People's Republic of China is chosen as the jurisdictional court, the stipulations on jurisdiction by level and exclusive jurisdiction in this Law shall not be contravened'.
92 The Provisional Regulations of the People's Republic of China Governing the Management of Computer Information Networks Hooked Up With International Networks, available at http://www.fas.org/irp/world/china/docs/internet_960201.htm (last visited on 31 August 2007).
93 Computer Information Network and Internet Security, Protection and Management Regulations, available at http://www.woodmedia.com/cinfolink/netregs.htm (last visited on 31 August 2007).
94 According to the related law, whatever their nationality, a lawsuit will be sued in the court of the state of the defendant's domicile. In order to determine whether a party is domiciled in a contracting state, a court shall apply its domicile; in order to determine that seat the court shall apply its rules of private international law. For example, if the defendant's domicile is China, the Chinese Court will apply the internal law rules and related Chinese private international law to determine the domicile.
95 That is Nationality Principle.
96 Articles 244–45 of the Civil Procedure Law of the People's Republic of China.
97 The Civil Procedure Law of the People's Republic of China provides a plaintiff with a choice where he may sue the defendant. The plaintiff can choose the place where the contract should be performed, or the place where the contract was signed or executed, or of the distrainable property, or of the place where the infringing conduct took place or where the representative office is located, to be the forum.
98 Article 246 of the Civil Procedure Law of the People's Republic of China.
99 It means China has jurisdiction over crimes happening within Chinese territory.
100 Tan (2001).
101 Fawcett, Harris & Bridge (2005), p. 594.
102 Article 3(1) of the EC Directive on Electronic Commerce.
103 Recital 21 of the EC Directive on Electronic Commerce.
104 Fawcett, Harris & Bridge (2005), p. 1233.
105 The Convention on the Law Applicable to Contractual Obligations (The Rome

Convention 1980), latest consolidated version, 30.12.2005, Official Journal of the European Union, C334/1.

106 Proposal for a Regulation of the European Parliament and the Council on the Law Applicable to Contractual Obligations (Rome I), Brussels, 15.12.2005, COM(2005) 650 final 2005/0261 (COD).

107 'Adoption of two Commission Proposals is a vital step in completing the European law – enforcement area for individuals and firms', IP/05/605, Brussels, 15 December 2005.

108 Regulation (EC) No 593/2008 of the European Parliament and the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), OJ L 177/6–16, 4 July 2008.

109 Article 24(1) of the Rome I Regulation.

110 Article 28 of the Rome I Regulation.

111 OJ L 12, 16.1.2001, p. 1.

112 Wilderspin (2008).

113 Hill (2005), p. 481.

114 Giuliona–Lagarde Report, [1980] OJ C282/1, p. 17.

115 Lando (1987), pp. 159, 168.

116 McLachlan (1990), p. 311.

117 Hill (2005), p. 482.

118 Article 14 of the UN Convention on the Use of Electronic Communications in International Contracts (the UN Convention).

119 'Green Paper on the Conversion of the Rome Convention of 1980 on the law applicable to contractual obligations into a Community instrument and its modernisation' (hereafter Green Paper), COM (2002) 654 final, Brussels 14.1.2003, Commission of the European Communities, p. 25, available at http://eur-lex.europa.eu/LexUriServ/site/en/com/2002/com2002_0654en01.pdf (last visited on 25 August 2007).

120 Proposal for the Rome I Regulation, p. 5.

121 Article 4(1) of the Rome I Regulation.

122 Article 4(1)(a) of the Rome I Regulation.

123 Article 4(4) of the Rome I Regulation.

124 'Green Paper on the Conversion of the Rome Convention of 1980 on the law applicable to contractual obligations into a Community instrument and its modernisation', COM (2002) 654 final, Brussels 14.1.2003, Commission of the European Communities, available at http://eur-lex.europa.eu/LexUriServ/site/en/com/2002/com2002_0654en01.pdf (last visited on 25 August 2007).

125 According to Article 9 of the Rome Convention, it governs formal validity by providing:

1. A contract concluded between persons who are in the same country is formally valid if it satisfies the formal requirements of the law which governs it under this Convention or of the law of the country where it is concluded.
2. A contract concluded between persons who are in different countries is formally valid if it satisfies the formal requirements of the law which governs it under this Convention or of the law of one of those countries.
3. Where a contract is concluded by an agent, the country in which the agent acts is the relevant country for the purposes of paragraphs 1 and 2.
4. An act intended to have legal effect relating to an existing or contemplated contract is formally valid if it satisfies the formal requirements of the law which under this Convention governs or would govern the contract or of the law of the country where the act *was done*.

126 Document 373–33/8, p. 6; 'Response of the Government of the United Kingdom',

p. 8, available at http://ec.europa.eu/justice_home/news/consulting_public/rome_i/doc/united_kingdom_en.pdf (last visited on 25 August 2007).

127 Green Paper, p. 39, COM (2002) 654 final, Brussels 14.1.2003.
128 Article 10(3) of the UN Convention.
129 *Ibid*, Article 6(3).
130 As stated in the Green Paper, 'It will be enough, therefore, for the statement to satisfy the formal requirements of one of the three laws to be valid as to form. This rule will apply without discrimination to contracts concluded by electronic means and to other contracts concluded at a distance', p. 39, COM(2002) 654 final, Brussels 14.1.2003.
131 Article 11 of the Rome I Regulation.
132 Article 10 (1) and (2) of the Proposal for a Regulation of the European Parliament and of the Council on the law applicable to contractual obligations (Rome I), Council of the European Union, 13853/06, LIMITE, JUSTCIV 224, CODEC 1085, Brussels, 12 October 2006.
133 Employed from Article 3(c) of the Choice of Court Convention.
134 Article 4(1)(a) of the Rome I Regulation.
135 §103 of UCITA.
136 Scoles, Hay, Borchers & Symeonides (2000), p. 858.
137 *Ibid*, p. 861.
138 (2) The law of the state chosen by the parties to govern their contractual rights and duties will be applied, even if the particular issue is one which the parties could not have resolved by an explicit provision in their agreement directed to that issue, unless either (a) the chosen state has no substantial relationship to the parties or the transaction and there is no other reasonable basis for the parties' choice, or (b) application of the law of the chosen state would be contrary to a fundamental policy of a state which has a materially greater interest than the chosen state in the determination of the particular issue and which, under the rule of §188, would be the state of the applicable law in the absence of an effective choice of law by the parties.
139 Mazzotta (2001), pp. 249, 252.
140 *Vita Food Products Inc. v Unus Shipping Co. Ltd* [1939] AC 277.
141 Yeo (2004), p. 1.
142 Rice (2000), p. 608.
143 Article 9(4) of the UN Convention.
144 §6 of the Second Restatement – the Choice of Law Principles:

(1) A court, subject to constitutional restrictions, will follow a statutory directive of its own state on choice of law.
(2) When there is no such directive, the factors relevant to the choice of the applicable rule of law include

(a) the needs of the interstate and international systems,
(b) the relevant policies of the forum,
(c) the relevant policies of other interested states and the relative interests of those states in the determination of the particular issue,
(d) the protection of justified expectations,
(e) the basic policies underlying the particular field of law,
(f) certainty, predictability and uniformity of result, and
(g) ease in the determination and application of the law to be applied.

145 Except as otherwise provided in §189–99 and 203, provided by §188(3) of the Second Restatement.
146 Scoles, Hay, Borchers & Symeonides (2000), p. 898.
147 *Sander v Doe*, 831 F.Supp. 886 (S.D.Ga.1993).

148 *International Harvester Credit Corp. v Risks.*, 16 N.C. App. 491, 192 S.E. 2d 707 (1972).
149 *McLouth Steel Corp. v Jewell Coal & Coke Co.* 570 F. 2d 594, 601 (6th Cir. 1978), cert. dismissed 439 U.S. 801, 99 S. Ct. 43, 58 L.Ed.2d 94 (1978).
150 §109(a) of the UCITA provides: '(1) An access contract or a contract providing for electronic delivery of a copy is governed by the law of the jurisdiction in which the licensor was located when the agreement was entered into.(2) A consumer contract that requires delivery of a copy on a tangible medium is governed by the law of the jurisdiction in which the copy is or should have been delivered to the consumer'.
151 'Location of the Parties', provided by Article 6 of the UN Convention.
152 §109 (c) of the UCITA.
153 UCITA with prefatory note and comments, available at http://www.law.upenn.edu/bll/ulc/ucita/2002final.htm (last visited on 30 April 2007).
154 Zhang (2006), pp. 289, 297.
155 Zhang (2006), pp. 289, 298; See also Article 178 of Organic Law of the People's Courts, promulgated by the National People's Congress in 1979.
156 China National People's Congress, Public Notice 1999 No 14.
157 Article 126 of the Contract Law of the People's Republic of China 1999 (hereafter the Chinese Contract Law), available at http://cclaw.net/ (last visited on 27 August 2007).
158 General Principles of Civil Law of the People's Republic of China, promulgated on 12 April 1986, Articles 142–50.
159 Article 126 of the Chinese Contract Law.
160 *Ibid*.
161 Zhang (2006), pp. 289, 325.
162 See Supreme People's Court, The Answers to Questions about Application of The Foreign Economic Contract Law of China (1987).
163 Ponte (2001), 55, p. 60–61.
164 Katsh & Rifkin (2001), p. 10.
165 American Bar Association Task Force on E-Commerce and ADR, 'Addressing Disputes in Electronic Commerce, Final Report and Recommendation', available at http://www.abanet.org/dispute/documents/FinalReport102802.pdf (last visited on 29 July 2008).
166 Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the application of Council Regulation (EC) No 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, Brussels, 21.4.2009, COM(2009) 174 final, Commission of the European Communities, p. 9, available at http://www.ipex.eu/ipex/cms/home/Documents/doc_COM20090174FIN (last visited on 18 June 2009).
167 Green Paper on the Review of Council Regulation (EC) No 44/2001 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, Brussels, 21.4. 2009, COM(2009) 175 final, Commission of the European Communities, p. 8, available at http://www.ipex.eu/ipex/cms/home/Documents/doc_COM20090175FIN (last visited on 18 June 2009).
168 EC Directive of the European Parliament and of the Council on Certain Aspects of Mediation in Civil and Commercial Matters, Brussels, 28 February 2008, 15003/5/07 REV5, available at http://ec.europa.eu/civiljustice/docs/st15003-re05_en07.pdf (last visited on 21 May 2008).
169 Directive 2008/52/EC of the European Parliament and of the Council of 21 May 2008 on certain aspects of mediation in civil and commercial matters, L136/5, Official Journal of the European Union, 24.5.2008, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:136:0003:0008:EN:PDF (last visited on 25 May 2008).

170 EU Press Release Reference: Mediation in civil and commercial matters, MEMO/08/263, Brussels, 23/04/2008, available at http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/08/263&type=HTML&aged=0&language=EN&guiLanguage=en (last visited on 25 May 2008).
171 Wang (2008a), p. 44.
172 Recitals (8) and (9) of the Mediation Directive 2008.
173 Article 4 of the Mediation Directive 2008.
174 Article 9 of the Mediation Directive 2008.
175 Article 17(1) of the EC Directive on Electronic Commerce.
176 *Ibid*, Article 17(2).
177 *Ibid*, Article 17(3).
178 ABA ODR Survey (2002).
179 ABA ODR Survey (2002), pp. 415, 444.
180 ABA Model Standards of Conduct for Mediators, September 2005, available at http://www.abanet.org/dispute/documents/model_standards_conduct_april2007.pdf (last visited on 19 June 2009).
181 Article 10 of the Arbitration Law of the People's Republic of China, Adopted at the 8th Session of the Standing Committee of the 8th National People's Congress and promulgated on August 31, 1994, available at http://english.sohu.com/2004/07/04/78/article220847885.shtml (last visited on 4 September 2007).
182 Article 13 of the Arbitration Law of the People's Republic of China.
183 *Ibid*, Article 11.
184 Article 1 of the CIETAC Online Arbitration Rules 2009.
185 Tao (2005), pp. 1,012–1,013.
186 It was adopted at the Fourth Session of the Seventh National People's Congress on 9 April 1991, promulgated and effective by Order No.44 of the President of the People's Republic of China as of 9 April 1991.
187 It was adopted at the Eighth Session of the Standing Committee of the Eighth National People's Congress and promulgated on 31 August 1994 and effective as of 1 September 1995.
188 It was adopted by the First Session of the Standing Committee of the Seventh National People's Congress on 13 April 1988, promulgated and revised by the Eighteenth Session of the Standing Committee on the Ninth National People's Congress on 31 October 2000.
189 1958 – Convention on the Recognition and Enforcement of Foreign Arbitral Awards, status, available at http://www.uncitral.org/uncitral/en/uncitral_texts/arbitration/NYConvention_status.html (last visited on 19 June 2009).
190 Dispute Resolution Overview, available at http://pages.ebay.com/services/buyandsell/disputeres.html (last visited on 19 June 2009).
191 *Ibid*.
192 About us (AAA), available at http://www.adr.org/about (last visited on 19 June 2009).
193 Information about AAA and Cybersettle Sign Unique Partnership Agreement, available at http://www.cybersettle.com/pub/16/section.aspx/11 and http://www.cybersettle.com/pub/home/about/partners/aaa.aspx & http://www.adr.org/sp. asp?id=32533 (last visited on 19 June 2009).
194 Industry New: New Joint Dispute Resolution Service Ready to Launch, available at http://www.adr.org/sp. asp?id=29624 (last visited on 19 June 2009).
195 The Internet Corporation for Assigned Names and Numbers (ICANN), available at http://www.icann.org/ (last visited on 29 May 2008).
196 'What is WIPO?', available at http://www.wipo.int/about-wipo/en/what_is_wipo.html (last visited on 19 June 2009).
197 The WIPO Arbitration and Mediation Centre, available at http://www.wipo.int/amc/en/index.html (last visited on 29 May 2008).

198 Frequently Asked Questions: Internet Domain Names, available at http://www.wipo.int/amc/en/center/faq/domains.html (last visited on 29 May 2008).
199 WIPO Advanced Workshop on Domain Name Dispute Resolution: Update on Practices and Precedents, WIPO, Geneva, Switzerland, Tuesday and Wednesday, 13 and 14 October 2009, available at http://www.wipo.int/amc/en/events/workshops/2009/domainname/ (last visited on 19 June 2009).
200 WIPO eUDRP Initiative, available at http://www.wipo.int/export/sites/www/amc/en/docs/icann301208.pdf (last visited on 19 June 2009).
201 Record Number of Cybersquatting Cases in 2008, WIPO Proposes Paperless UDRP, PR/2009/585, Geneva, 16 March 2009, available at http://www.wipo.int/pressroom/en/articles/2009/article_0005.html (last visited on 19 June 2009).
202 Motion (2005), pp. 137–69, 148.
203 WIPO UDRP Domain Name Decision (gTLD), available at http://www.wipo.int/amc/en/domains/decisionsx/index.html (last visited on 19 June 2009).
204 Paragraph 4(k) of the UDRP Policy.
205 Case Filing under the UDRP, available at http://www.wipo.int/amc/en/domains/filing/udrp/index.html (last visited on 19 June 2009).
206 Asian Domain Name Dispute Resolutions Centre, http://www.adndrc.org/adndrc/index.html (last visited on 19 June 2009). Please note that it also includes the Korean Internet Address Dispute Resolution Committee (KIDRC).
207 CIETAC Domain Name Dispute Resolution Centre, available at http://dndrc.cietac.org/static/english/engfrmain.html (last visited on 19 June 2009).
208 HKIAC .cn Domain Name Resolution Centre, available at http://dn.hkiac.org/cn/cne_welcome.html (last visited on 19 June 2009).
209 The China Internet Information Centre (CNNIC) approved and implemented the CNNIC Domain Name Dispute Resolution Policy (CNDRP) on 30 September 2002. The new amended CNDRP came into force on 17 March 2006.
210 Hong Kong International Arbitration Centre (HKIAC), http://dn.hkiac.org/cn/cne_complaint_form.html (last visited on 24 May 2008).
211 Article 37 of the Rules for CNNIC Domain Name Dispute Resolution Policy, available at http://dn.hkiac.org/cn/cne_rules_procedure.html (last visited on 25 May 2008).
212 Article 44 of the Rules for CNNIC Domain Name Dispute Resolution Policy, available at http://dn.hkiac.org/cn/cne_rules_procedure.html (last visited on 25 May 2008).
213 *Avon Products, INC. v Ni Ping*, CN-0600087, available at http://www.adndrc.org/adndrc/bj_statostocs.html (last visited on 27 March 2007).
214 Dispute Resolution Overview, available at http://pages.ebay.com/services/buyandsell/disputeres.html (last visited on 19 June 2009).
215 *Ibid*.
216 Calliess (2006), pp. 647, 653.
217 In the author's view, 'social-legal bonds' means the combination of the powers between social organisations and legislation. The term 'legal bond' is being used in a very broad sense, including not only contractual design but also all kinds of 'private ordering', see more details in http://odrworkshop. info/papers2005/odrworkshop2005Bol.pdf (last visited on 29 July 2008).
218 Available at http://www.icann.org/tlds/agreements/name/registry-agmt-appl-03jul01.htm (last visited on 3 September 2007).
219 A Review of the Relationship between Trade Marks and Business Names, Company Names and Domain Names (March 2006), Australian Government, Advisory Council on Intellectual Property, p. 5, available at http://www.acip. gov.au/library/TM,%20business,company,domain%20names%20Final%20Report.pdf (last visited on 17 March 2007), hereafter Australian DR Review.

220 Tunkel & York (2000).
221 Wang (2006), pp. 116–27, 119.
222 Efroni (2002), p. 343.
223 Wang (2008a), p. 61.
224 Katsh & Rikfin (2001), p. 76.
225 *Brown v Rice* [2007] EWHC 625 (Ch); [2007] BPIR 305 (Ch D).
226 Recital 19 and Article 6 of the Mediation Directive 2008.
227 *Ibid*, Article 6(2).
228 *Ibid*, Recital 23 and Article 7.
229 *Ibid*, Article 7(1).
230 Rabinovich-Einy (2006), p. 256.
231 Square Trade Privacy Policy, available at http://www.squaretrade.com/cnt/jsp/lgl/user_conf_agree.jsp?vhostid=chipotle&stmp=squaretradeconf_infocollect (last visited on 29 November 2006).
232 'Recommended Best Practices by Online Dispute Resolution Service Providers', available at http://www.abanet.org/dispute/documents/BestPracticeFinal102802.pdf (last visited on 18 June 2009).
233 Rabinovich-Einy (2006), pp. 253, 259.

11 Conclusions and recommendations

1 Dalhuisen (2007), p. 254.
2 Article 10 of the UN Convention on the Use of Electronic Communications in International Contracts.
3 Article 6 of the UN Convention.

References

Aciman, C. & D. Vo-Verde (2002) 'Refining the Zippo Test: New Trends on Personal Jurisdiction for Internet Activities', 19 *Computer & Internet Law*, 16.

Akdeniz, Y., Clarke, O., Kelman, A. & Oram, A. (1997) 'Cryptography and Liberty: Can the Trusted Third Parties be Trusted? A Critique of the Recent UK Proposals', 2 *The Journal of Information, Law and Technology* at http://elj.warwick.ac.uk/jilt/cryptog/97_2akdz/ (last visited on 4 July 2004).

Anderson, D. S. (2005) 'The 2005 Randoloph W. Thrower Symposium Families in the 21st Century: Changing Dynamics, Institutions, and Polices: Comment: What Trust is in These Times? Examining the Foundation of Online Trust', 54 *Emory L. J.* 1441.

Angel, J. (1999) 'Why use Digital Signature for Electronic Commerce?', 2 *The Journal of Information, Law and Technology* at http://elj.warwick.ac.uk/jilt/99-2/angel.html (last visited on 3 July 2004).

Bainbridge, D. I. (2008) *Introduction to Information Technology Law* (Harlow: Pearson Longman, 6th edn).

Baker, S. & Yeo, M. (1999) 'Survey of International Electronic and Digital Signature Initiatives', from Internet Law & Policy Forum Working Group, at http://www.ilpf.org/groups/survey.htm (last visited 2 August 2004).

Bartell, D. W. (2000) *E-contracts* (Ledbury: BWCS Ltd), p.208.

Basu, S. & Jones, R. (2003) 'E-commerce and the Law: A Review of India's Information Technology Act 2000', 12 (1) *Contemporary South Asia* 19.

Beecher, S. (2006) 'Can the Electronic Bill of Lading Go Paperless?', *International Lawyer*, 2006, Vol 40, No 3, pp.627–48.

Berman, P. S. (2002) 'The Globalization of Jurisdiction', 151 *U. Pa. L. Rev.* 311.

Bharvada, K. (2002) 'Electronic Signatures, Biometrics and PKI in the UK', 16(3) *International Review of Law Computers and Technology* 265–75.

Blythe, S. E. (2005) 'Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce with Enhanced Security', 11 *Rich. J. L. & Tech.* 6.

Boone, B. D. (2006) 'Bullseye!: Why a "Targeting" Approach to Personal Jurisdiction in the E-commerce Context Makes Sense Internationally', 20 *Emory Int'l L. Rev.* 241.

Boss, A. H. (1998) 'Electronic Commerce and the Symbiotic Relationship Between International and Domestic Law Reform', 72 *Tul. L. Rev.* 1931, 1933.

Burnett, R. & Klinger, P. (2005) *Drafting and Negotiating Computer Contracts* (Sussex: Tottel Publishing, 2nd edn), p.73.

Calliess, G. P. (2006) 'Online Dispute Resolution: Consumer Redress in a Global Market Place', Vol 07 No 08 *German Law Journal*, 647.

Campbell, C. E. & Berenstein, G. L. (2002) 'Electronic Contracting: The Current State of the Law and Best Practices', 14 No 9 *J. Proprietary Rts.* 1.

Capps, D. (2002) 'Conveyancing in the 21st Century: An outline of Electronic Conveyancing & Electronic Signatures', Sep/Oct CONVPL 443–55.

Carnabuci, C. & Li, J. (2005) 'China: Electronic Commerce – Legislation', *C.T.L.R.* 11(6) N69.

Chan, F. W. H. (2005) 'China's Electronic Signature Act 2005: A Great Leap Forward or Backward', *C.T.L.R.* 11(2) 47–50.

Chen, F. (2001) 'The New Era of Chinese Contract Law: History, Development and a Comparative Analysis', *27 Brooklyn J. Int'l L.* 153, 173.

Chik, W. B. (2002) 'U.S. Jurisdictional Rules of Adjudication Over Business Conducted Via the Internet-Guide-lines and a Checklist for the E-Commerce Merchant', 10 *Tul. J. Int'l & Comp. L.* 243, 248–49.

Cooper, D., Fink, D., Jones, E., and Quathem, K. V. (2006) Security Breach Notification in Europe on the Horizon, World Data Protection Report, October 2006, available at http://www.cov.com/files/Publication/69e65c7e-4d08-474e-853b-3635e9120777/Presentation/PublicationAttachment/4064434a-7a6e-419e-8996-3c810d88da9c/757.pdf (last visited on 15 June 2009).

Craig, W. J. (2004) Hague Conference on E-Commerce Law, Introductory and Background Issues, Hague E-Commerce Conference, 26–27 October 2004, available at http://hcch.e-vision.nl/upload/wop/e-comm_craig.pdf (last visited on 3 September 2007).

Dalhuisen, J. H. (2007) *Dalhuisen on Transnational and Comparative Commercial, Financial and Trade Law* (Oxford and Portland, Oregon: Hart Publishing, 3rd edn).

Del Duca, L. F. (2005–06) 'Implementation of Contract Formation, Statute of Frauds, Parol Evidence, and Battle of Forms CISG Provisions in Civil and Common Law Countries', 25 *Journal of Law and Commerce* 133, originally published in (2005) 38 *UCC L. J.* 55.

Deveci, H. A. (2006) 'Personal Jurisdiction: Where cyberspace meets the real world – Part II', *Computer Law & Security Report* 22, 39–45.

Diedrich, F. (2000) 'A Law of the Internet? Attempts to Regulate Electronic Commerce', 3 *The Journal of Information, Law and Technology* at http://elj.warwick.ac.uk/jilt/00-3/diedrich.html (last visited on 3 November 2004).

Efroni, Z. (2002) 'The Anticybersquatting Consumer Protection Act and the Uniform Dispute Resolution Policy: New opportunities for international forum shopping?', *Columbia Journal of Law & the Arts*, 26, 335–43.

Faria, J. A. E. (2006) 'The United Nations Convention on the Use of Electronic Communications in International Contracts – An Introductory Note', *International and Comparative Law Quarterly* Vol 55, 689–94.

Fawcett, J. J., Harris, J. M. & Bridge, M. (2005) *International Sale of Goods in the Conflict of Laws* (New York: Oxford University Press).

Forte, A. D. M. (2006) 'The Battle of Forms' in MacQueen, H.L. & Zimmermann, R. (eds), *European Contract Law: Scots and South African Perspectives* (Edinburgh: Edinburgh University Press), 98–122.

Fresen, G. W. (1997) 'What lawyers should know about digital signatures', 85 *Ill. B. J.* 170, 171.

Froomkin, A. M. (1996) 'The Essential Role of Trusted Third Parties in Electronic Commerce', 1 (75) *Oregon L. Rev.* 49 at http://www.law.miami.edu/froomkin/articles/trusted1.htm (last visited on 30 July 2004).

Gardner, S. (1992) 'Trashing with Trollope, A deconstruction of the Postal Rule in Contract', *Oxford Journal of Legal Studies* 170.

Geist, M. (2001) 'Is There a There There? Toward Greater Certainty for Internet Jurisdiction', 661 *PLI/PAT* 561, 575; 16 *Berkeley Tech. L.J.* 1345, 1362.

Ghoshray, S. (2005) 'Symposium: The Common Law of Contracts as a World Force in Two Ages of Revolution: A Conference Celebrating the 150th Anniversary of Hadley v. Baxendale: The Boundaries of Contract in a Global Economy: Cyberspace Contracting: Embracing Incomplete Contract Paradigm in the Wake of UCITA Experience', 11 *Tex. Wesleyan L. Rev.* 609.

Girvin, S. (2007) *Carriage of Goods by Sea* (Oxford: Oxford University Press), pp.162–63.

Gladstone, J. (1997) 'Designing Legislation to Facilitate Electronic Commerce on the Internet', 45 *R.I.B.J.* 13.

Goode, R. (1997) 'Usage and its Reception in Transnational Commercial Law', *International & Comparative Law Quarterly* Vol 46, pp.1–36, 3.

Gringras, C. (2003) *Laws of the Internet* (London: Butterworths, 2nd edn).

Guest, A. G. *et al.* (eds) (1989) *Chitty on Contracts – General Principles* (London: Sweet & Maxwell, 26th edn).

Hill, J. (2005) *International Commercial Disputes in English Courts* (Oxford & Portland, Oregon: Hart Publishing, 3rd edn).

Hindelang, S. (2002) 'No Remedy for Disappointed Trust – The Liability Regime for Certification Authorities Towards Third Parties Outwith the EC Directive in England and Germany Compared', 1 *The Journal of Information, Law and Technology* at http://elj.warwick.ac.uk/jilt/02-1/hindelang.html (last visited on 9 June 2004).

Julia-Barcelo, R. & Vinje, T. C. (1998) 'Another Step Towards A European Framework For Electronic Signatures: The Commission's Directive Proposal', 14(5) *Computer Law & Security Report* 303.

Katsh, E. M. & Rifkin, J. (2001) *Online Dispute Resolution: Resolving Conflicts in Cyberspace* (San Francisco: Jossey-Bass).

Kidd, Jr, D. L. & Daughtrey, Jr, W .H. (2000) 'Adopting Contact Law to Accommodate Electronic Contracts: Overview and Suggestions', 26 *Rutgers Computer & Tech. L. J.* 215.

Kuner, C. (2003) *European Data Privacy Law and Online Business* (New York: Oxford University Press).

Lando, O. (1987) 'The EEC convention on the law applicable to contractual obligations', *Common Market Law Review*, 24, 159–214.

Leng, T. K. (2006) 'Note and Comments: Towards Uniform Electronic Contracting Law', 18 *Singapore Academy of Law Journal* 234.

Lessig, L. (2001) 'Preface to a Conference on Trust', 81 *B.U.L.Rev.* 329.

Lloyd, I. (2000) *Legal Aspects of Information Society* (London, Edinburgh, Dublin: Butterworths).

Lloyd, I. J. (2004) *Information Technology Law* (Oxford: Oxford University Press, 4th edn).

Maloney, M. (1993) 'Specific Jurisdiction and the "Arise from or Relate to" Requirement . . . What Does it Mean?', 50 *Wash. & Lee. L. Rev.* 1265.

Mann, R. J. & Winn (2005) *Electronic Commerce* (New York: Aspen Publishing, 2nd edn), p.193.

Maxeiner, J. R. (2003) 'Standard Terms Contracting in the Global Electronic Age: European Alternatives', 28 *Yale Journal of International Law* 109.

Mazzotta, F. G. (2001) 'A Guide to E-Commerce: Some Legal Issues Posed by E-Commerce for American Businesses Engaged in Domestic and International Transactions', *24 Suffolk Transnat'l L. Rev.* 249.

Mckay, Jr. J. C. (July/August 2000) UETA, UCITA, and E-Sign: A Preliminary Comparison, 5 *Cyberspace Lawyer*, 20.

McLachlan, C. (1990) 'Splitting the Proper Law in Private International Law' (1990) 61 *BYIL* 311.

Mootz, F. J. (2007) 'After the Battle of the Forms: Commercial Contracting in the Electronic Age', available at http://ssrn.com/abstract=981288 (last visited on 30 April 2007).

Moreno, C. (2001) 'Brief Overview of Selective Legal and Regulatory Issues in Electronic Commerce' at International Symposium on Government and Electronic Commerce Development, Ningbo (China), 23–24 April 2001 at http://unpan1.un.org/intradoc/groups/public/documents/un/unpan001099.pdf (last visited on 1 July 2009).

Morris, McClean, D. & Beevers, K. (2005) *The Conflict of Laws* (London: Sweet & Maxwell Ltd, 6th edn).

Motion, P. (2005) 'Article 17 ECD: Encouragement of Alternative Dispute Resolution On-line Dispute Resolution: A View From Scotland', pp.137–69 in Edwards, L. (ed.), *The New Legal Framework for E-commerce in Europe* (Oxford: Hart Publishing).

Murray, A. D. (2000a). 'Entering into Contracts Electronically: The Real WWW', pp.17–35, in Edwards, L. & Waelde, C. (eds) *Law and the Internet: A Framework for Electronic Commerce* (Oxford: Hart Publishing).

Murray, J. E. (2000b) 'The Definitive "Battle of the Forms": Chaos Revisited' (2000) 20 *J.L. & COM.* 1.

Murray, J. (2003) 'Public Key Infrastructure Digital Signatures and Systematic Risk', 1 *The Journal of Information, Law and Technology* at http://elj.warwick.ac.uk/jilt/03-1/murray.html (last visited on 3 November 2004).

ODR Survey (2002) 'Survey: Addressing Disputes in Electronic Commerce: Final Recommendations and Report', 58 *Bus. Law*, 415, produced by the American Bar Association's Task Force on Electronic Commerce and Alternative Dispute Resolution in Cooperation with the Shidler Center of Law, Commerce and Technology, University of Washington School of Law.

Ong, R. (2004) 'Consumer Based Electronic Commerce: A Comparative Analysis of the Position in Malaysia and Hongkong', 12 *Int'l J.L. & Info. Tech.* 101.

Osty, M. J. & Pulcanio, M. J. (1999) 'The Liability of Certification Authorities to Relying Third Parties', 17 *J. Marshall J. Computer & Info. L.* 961, available at http://www.jcil.org/journal/articles/220.html (last visited on 3 September 2007).

Pappas, C. W. (2002) 'The Holland & Hart Private International Law Award: Comparative U.S. & EU Approaches to E-commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures and Taxation', *31 Denv. J. Int'l L. & Pol'y* 325, 331.

Ponte, L. M. (2001) 'Throwing Bad Money After Bad: Can Online Dispute Resolution

(ODR) Really Deliver the Goods for the Unhappy Internet Shopper?' 3 *Tul. J. Tech. & Intell. Prop.* 55.

Qin, C. D. (2008) *Electronic Commerce Law* (Xi'an: Xi'an JiaoTong Univeristy Press), pp.234, 249.

Rabinovich-Einy, O. (2006) 'Technology's Impact: the Quest for a New Paradigm for Accountability in Mediation', 11 *Harv. Negot. L. Rev.* 253.

Ramberg, C. H. (2001) 'The E-commerce Directive and Formation of Contract in a Comparative Perspective', Vol 1, Issue. 2, *Global Jurist Advances*, 3.

Recktenwald, J. (2004) 'Electronic Authentication Technology Takes Off' at http://www.cybersign.com/TechRepublic.htm (last visited on 22 August 2004).

Rice, D. T. (2000) 'Jurisdiction in Cyberspace: Which Law and Forum apply to Securities Transactions on the Internet?', 21 *U. Pa. J. Int'l Econ. L.* 585.

Rice, D. T. (2004) 'Problems in Running a Global Internet Business: Complying with the Laws of Other Countries', 797 *PLI/PAT* 11, 52.

Rice, D. T. & Gladstone, J. (2003) 'An Assessment of the Effects Test in Determining Personal Jurisdiction in Cyberspace', 58 *Bus. Law.* 601.

Robinson, N., Graux, H., Botterman, M. & Valeri, L. (2009), Review of EU Data Protection Directive: Summary, prepared for the Information Commissioner's Office, available at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive_summary.pdf (last visited on 12 June 2009).

Rosner, N. (2004) 'International Jurisdiction in European Union E-Commerce Contracts' in Kinsella, N. S. & Simpson, A. F. (eds), *Online Contract Formation* (New York: Oceana Publications, Inc.), p.481.

Ryssdal, R. (1991) Data Protection and the European Convention on Human Rights, XIII CONF. DATA PROTECTION COMM'RS 39.

Savirimuthu, J. (2005) 'Online Contract Formation: Taking Technological Infrastructure Seriously', 2 *UOLTJ* 105.

Scoles, E. F., Hay, P., Borchers, P. J. & Symeonides, S. C. (2000) *Conflict of Laws* (St. Paul, Minn.: West Group, 3rd edn).

Smedinghoff, T. J. (1996) *Online Law: The SPA's Legal Guide to Doing Business on the Internet* (Addison-Wesley Developers Press), p.46.

Smith, G. J. H. (2002) *Internet Law and Regulation* (London: Sweet & Maxwell, 3rd edn), p.276.

Spyrelli, C. (2002) 'Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication' (2002) 2 *The Journal of Information, Law and Technology* at http://elj.warwick.ac.uk/jilt/02-2/spyrelli.html (last visited on 3 November 2004).

Stemp, K. C. (2005) 'A Comparative Analysis of the "Battle of the Forms" ', 15 *Transnational Law & Contemporary Problems* 243.

Stone, R. (2005) *The Modern Law of Contract* (London: Cavendish Publishing Limited, 6th edn).

Stuckey, K. D. (2005) *Internet and Online Law* (New York: ALM Properties, Inc., Law Journal Press), §1.02.

Swindells, C. & Henderson, K. (1998) 'Legal Regulation of Electronic Commerce', 3 *The Journal of Information, Law and Technology* at http://elj.warwick.ac.uk/jilt/98-3/swindells.html (last visited on 3 December 2004).

Tan, P. (2001) 'E-com Legal Guide Hongkong' at Baker & McKenzie at http://www.bakerinfo.com/apec/hongkong_main.htm (last visited on 6 February 2005).

Tao, J. (2005) *Resolving Business Disputes in China, Asia Business Law Series* (Netherlands: Kluwer Law International).

Terrett, A. & Monaghan, I. (2000) 'The Internet – An Introduction for Lawyers' in Edwards, L. & Waele, C. (eds), *Law and the Internet: A Framework for Electronic Commerce* (Oxford: Hart Publishing, 2nd edn).

Torre, C. & Allen, G. (2006) 'The Battle of the Forms – There is a Purpose', Volume 23, Issue 2 *Journal of Legal Studies Education* 195–216.

Tosto, N. D. & Baracks, B. (1996) 'Requirements for a Trusted Global Public Key Initiative', Vol 1, No 1 *Information Security Technical Report* 27.

Tunkel, D. & York, S. (2000) *E-commerce: A guide to the law of electronic business* (London: Butterworths, 2nd edn).

Wacks, R. (2001) 'Privacy Reconceived: Protecting Personal Information in a Digital World', in Lederman, E. and Shapira, R. (eds), *Law, Information and Information Technology* (Netherlands: Kluwer Law International), pp.75–97, 80.

Wang, F. (2006) 'Domain Names Management and Legal Protection', Vol 26, Issue 2, *International Journal of Information Management* 116–27.

Wang, F. (2008) 'Obstacles and Solutions to Internet Jurisdiction: A Comparative Analysis of the EU and US laws', *Journal of International Commercial Law and Technology*, Vol 3, Issue 4, pp.233–41, 241.

Wang, F. (2008a) *Online Dispute Resolution: Technology, Management and Legal Practice from an International Perspective* (Oxford: Chandos Publishing), p.44.

Wang, F. (2008b) 'E-Confidence: Offer and Acceptance in Online Contracting', Vol 22, No 3, *International Review of Law, Computers and Technology* 271–78.

Watnick, V. (2004) 'The Electronic Formation of Contracts and the Common Law Mailbox Rules', 56 *Baylor L. Rev.* 175.

Wei, C. K. & Suling, J. C. (2006) 'United Nations Convention on the Use of Electronic Communications in International Contracts – A New Global Standard', 18 *Singapore Academy of Law Journal* 116–202.

Wild, C., Weinstein, S. & MacEwan, N. (2005) *Internet Law* (London: Old Bailey Press).

Wilderspin, M. (2008) 'The Rome I Regulation: Communitarisation and Modernisation of the Rome Convention', ERA Forum 9: 259–74.

Wu, R. (2000) 'Electronic Transactions Ordinance – Building a Legal Framework for E-commerce in Hong Kong', 2000 (1) *The Journal of Information, Law and Technology* at http://elj.warwick.ac.uk/jilt/00-1/wu.html (last visited on 27 November 2004).

Yeo, T. M. (2004) *Choice of Law for Equitable Doctrines* (New York: Oxford University Press).

Zhang, C. & Lei, L. F. (2005) 'The Chinese Approach to Electronic Transactions Legislation', 9 *Computer L. Rev. & Tech. J.* 333, 335.

Zhang, M. (2006) 'Choice of Law in Contracts: A Chinese Approach', 26 *Northwestern Journal of International Law and Business* 289.

Index