LAW OF ELECTRONIC COMMERCIAL TRANSACTIONS

Contemporary Issues in the EU, US and China

Second Edition

FAYE FANGFEI WANG

Law of Electronic Commercial Transactions

Second Edition

The development of new technologies provides new challenges to the interpretation and implementation of legislation in the information society. The recent deployment of service-oriented computing and cloud computing for online commercial activities has urged countries to amend existing legislation and launch new regulations. With the exponential growth of international electronic commercial transactions, a consistent global standard of regulating the legal effects of electronic communications, the protection of data privacy security and the effectiveness of Internet-related dispute resolution are motivating factors to build users' trust and confidence in conducting cross-border business and sharing their information online.

The second edition of this book continues taking a 'solutions to obstacles' approach and analyses the main legal obstacles to the establishment of trust and confidence in undertaking business online. In comparing the legislative frameworks of e-commerce in the EU, US, China and international organisations, the book sets out solutions to modernise and harmonise laws at the national, regional and international levels in response to current technological developments. It specifically provides information on the key legal challenges caused by the increasing popularity of service-oriented computing and cloud computing as well as the growing number of cross-border transactions and their relation to data privacy protection, Internet jurisdiction, choice of law and online dispute resolution. It considers how greater legal certainty can be achieved in contracts in cloud computing or service-oriented architecture environments.

The second edition of *Law of Electronic Commercial Transactions* is a clear and up-to-date account of a fast-moving area of study. It will be of great value to legislators, politicians, practitioners, scholars, businesses, individuals, and postgraduate and undergraduate students. It provides in-depth research into finding solutions to remove eight generic legal obstacles in electronic commercial transactions and offers insights into policy-making, law reforms, regulatory developments and self-protection awareness.

Dr Faye Fangfei Wang (王芳菲) is Senior Lecturer in Law at Brunel Law School, Brunel University (London), UK. She holds a PhD from the University of Southampton, an LLM from the University of Aberdeen, and an LLB and diploma in computer science and application from Guangdong University of Foreign Studies, China. She is the convenor of the Cyberlaw Section at the Society of Legal Scholars in the UK. She specialises in cyberlaw most particularly from the private law perspective, covering the topics of contract law, commercial law, private international law, online dispute resolution, privacy and data protection and digital IP Rights. She is also the author of the monograph *Internet Jurisdiction and Choice of Law* (Cambridge University Press, 2010).

Routledge Research in IT and E-Commerce Law

Titles in this series include:

Law of Electronic Commercial Transactions, 1st and 2nd Editions
Contemporary Issues in the EU, US and China
Faye Fangfei Wang

Online Dispute Resolution for Consumers in the European Union
Pablo Cortés

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

International Internet Law
Joanna Kulesza

The Domain Name Registration System
Liberalisation, Consumer Protection and Growth
Jenny Ng

Law of Electronic Commercial Transactions

Contemporary Issues in the EU, US and China

Second Edition

Faye Fangfei Wang

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First Edition 2010
Second Edition 2014
by Routledge
2 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

and by Routledge
711 Third Avenue, New York, NY 10017

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

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. – Second edition.
pages cm. – (Routledge research in information technology and e-commerce law)
Includes bibliographical references and index.
ISBN 978-0-415-82971-7 (hardback) – ISBN 978-0-415-83224-3 (pbk) – ISBN 978-0-203-62881-2 (ebk) 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 2014
343.09'944–dc23
2013029498

ISBN: 978-0-415-82971-7 (hbk)
ISBN: 978-0-415-83224-3 (pbk)
ISBN: 978-0-203-62881-2 (ebk)

Typeset in Baskerville
by Cenveo Publisher Services

Contents

Table of cases

EU (ECJ/CJEU) cases

US cases

China cases

Other cases

This page intentionally left blank

List of abbreviations

AAA	American Arbitration Association
AAAI	Association for the Advancement of Artificial Intelligence
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
BIS	Department for Business, Innovation and Skills
CAs	Certificate Authorities
CIETAC	China International Economic and Trade Arbitration Commission
CIF	Cost, Insurance and Freight
CISG	UN Convention on Contracts for the International Sale of Goods
CJEU	Court of Justice of the European Union
CMI	Committee Maritime International
CNDRP	CNNIC Domain Name Dispute Resolution Policy
CNNIC	China Internet Network Information Center
COPPA	Children's Online Privacy Protection Act
CPS	Certificate Practice Statement
CSP	Certification Service Providers
DDoS	Distributed Denial of Service (Attack)
ECJ	European Court of Justice
ECPA	Electronic Communications Privacy Act
EDPS	European Data Protection Supervisor
EPIC	Electronic Privacy Information Center
ERA	Academy of European Law
ESIGN	Electronic Signatures in Global and National Commerce Act
FOB	Free on Board
FRA	EU Agency for Fundamental Rights
FTC	Federal Trade Commission
GDP	Gross Domestic Product

GST	Goods and Services Tax
gTLD	Generic Top-Level Domain
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
ICDR	International Center for Dispute Resolution
ICO	Information Commissioner's Office
IDABC	Interoperable Delivery of European eGovernment Services to Public Administrations, Businesses and Citizens
IP	Intellectual Property
ISP	Internet Service Provider
KIDRC	Korean Internet Address Dispute Resolution Committee
N&A	Notice and Action
NIST	National Institute of Standards and Technology
NPC	National People's Congress (China)
NRA	National Regulatory Authority
NTD	Notice and Takedown
ODR	Online Dispute Resolution
OECD	Organisation for Economic Cooperation and Development
PECL	Principles of European Contract Law
P2P	Peer to Peer
PETs	Privacy-Enhancing Technologies
PICC	Principles of International Commercial Contracts
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PRC	People's Republic of China
QoS	Quality of Service
RCA	Recognised Certificate Authority
RPA	Relying Party Agreement
SLA	Service Level Agreement
SMEs	Small and Medium-Sized Enterprises
SNS	Social Networking Site
SOA	Service-oriented Architecture
SOC	Service-oriented Computing
T&C	Terms and Conditions
TCP/IP	Internet Protocol Suite
UCC	Universal Commercial Code
UCITA	Uniform Computer Information Transactions Act
UCP	Uniform Customs and Practice
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
URL	Uniform Resource Locator

UTC	Coordinated Universal Time
WIPO	World Intellectual Property Organisation
WIPO-UDRP	World Intellectual Property Organisation – Domain Name Dispute Resolution Policy

This page intentionally left blank

Part I
Introduction

This page intentionally left blank

1 Introduction

1.1 Law of electronic commercial transactions: purpose and structure of this book

> 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])

Electronic commercial transactions have become increasingly important since the late 1990s. With the functional development of automated computing systems in recent years, decision-making regarding the sale of goods or services can be done automatically between two international trading companies with standard terms without any human interaction. These automated systems can design and offer a most favourable sale package to the buyer based on the information that the buyer gives, history of choice preferences and other data sources that the seller collects such as market prices, currency exchange rates and new modules, etc. Once the supply matches the demand (it usually takes a few seconds), an international contract of sale will be automatically concluded by the automated trading systems. Although business could benefit from such a system in terms of convenience and efficiency, there is potential legal uncertainty with regard to the validity of automated electronic contracts. The first part of this book discusses these challenges to business and proposes solutions to substantive contract law issues in the online environment such as the validity of offer and acceptance by electronic means, the incorporation of terms and conditions into electronic B2B and B2C sale/service contracts, error in electronic communications and the battle of forms. Electronic contracting is one of the core subjects in electronic commerce as legal certainty is the basis of building trust in doing business online. It compares the most current international legislation – the United Nations

1 *Thornton* v. *Shoe Lane Parking* [1971] 2 QB 163 at 169.

Convention on the Use of Electronic Communications in International Contracts 2005 – with relevant legislation in the EU, US and China.

In order to identify contracting parties and their affixed documents in the online environment, forms of encryption have been utilised. Electronic signatures, authentication and certificates are not only used as means to determine the identification and integrity of an electronic document but also help ensure online safety. When automated decision-making systems are used by individuals, it may further challenge personal data privacy protection. Automated agents can make decisions for individuals based on the collected data – models of individuals' preferences. Under automated systems, personal data including a long history of individuals' activities, behaviours and habits will be analysed and processed. Individuals may be more vulnerable to attack, because the system contains personal data of increased sensitivity. Moreover, the growing popularity of the use of cloud computing can further change the way we work, communicate with each other and share information as it makes data/information available and accessible anywhere. The benefits of cloud computing are the intended outcomes of cost savings, speed improvement and mobile accessibility. Nevertheless, the deployment of such technology may involve higher risk, consume more energy[2] and cause legal complication. It is essential that the conduct of Certificate Authorities (CAs) is regulated as their services impact the quality and trust on electronic markets. In most countries both non-recognised and recognised CAs are allowed to provide electronic authentication services and even may have the same effects on certificates. The second main section of the book provides in-depth analysis of the valid forms of electronic signatures and authentication, the liability of CAs and the recognition of foreign certificates. It researches into best practices for data privacy protection taking into account the current regulatory development and the conditions of informed consent for processing personal data in the EU, US and China. It also provides primary research on key legal challenges faced by new technologies (such as cloud computing) and proposes possible solutions to establish greater legal certainty by recommending necessary legal measures on striking a balance among different rights and bringing consistency of protection in practice. It argues that international coordination and protocols may redress the balance between the free flow of data for stimulating economic globalisation and the protection of fundamental data privacy rights to expedite the process of increasing trust and confidence in doing business online. It argues that an appropriate 'notice and takedown' (NTD) mechanism may be an efficient means for the implementation of Internet-related rights protection prior to court litigation and out-of-court dispute resolution.

2 G. Cook (2012) 'How clean is your cloud?', April, Greenpeace International. Available at: http://www.greenpeace.org/international/Global/international/publications/climate/2012/iCoal/HowCleanisYourCloud.pdf (last accessed 30 June 2013).

In spite of the fact that there are modern Internet regulations, Internet-related disputes have unique characteristics that often challenge traditional legal concepts and procedural rules in court litigation and out-of-court dispute resolution. When digitised goods are delivered through electronic networks, the place of delivery is no longer physical, thus it is much more difficult to ascertain the place of delivery online than offline. Moreover, customers and users may not be able to choose or restrict the location of data centres prior to the conclusion of the Service Level Agreement (SLA) for cloud-computing services. Data centres may be relocated or added at any time and as a result they may be located in various jurisdictions which could contribute to the difficulty in identifying the location of infringement and determining the competent court and applicable law. This, leaving well alone other legal issues of cloud computing, furthers the existing challenges of Internet jurisdiction and choice of law for electronic commercial transactions which began in the early 2000s. The possibility of automated system-generated choice of court and choice of law agreements and online delivery of digitised goods may challenge the traditional principles of determining jurisdiction and applicable law. Subsequently it requires the interpretation or even amendment of the existing conflict of law rules so as to adapt to the contemporary information society in the transnational sphere. The third main part of the book investigates key factors for the determination of Internet jurisdiction and applicable law in the EU, US and China and examines general, special and exclusive jurisdiction rules accordingly. It attempts to find ways to remove obstacles to the determination of Internet jurisdiction and applicable law in cases of choice and in the absence of parties' choice. It undertakes primary research providing an overview of what pressure the growing popularity of new technologies places upon the validity of jurisdiction and applicable law clauses for electronic commercial contracts, and how the legal barriers can be removed. It seeks for a harmonised interpretation of jurisdictional factors to ensure fairness and legal certainty at the international level. It also argues that online dispute resolution (ODR) can be developed as a tailor-made first resort for civil and commercial Internet-related (in particular cross-border) disputes before court litigation and traditional alternative dispute resolution. It analyses most successful examples of ODR services and discusses the United Nations Commission on International Trade Law (UNCITRAL) working group draft ODR procedural rules for cross-border electronic commerce transactions in comparison with the current legislative development in the EU (EU Regulation on Consumer ODR 2013), US and China. It concludes that ODR may become one of the possible and most efficient channels to enhance trust and confidence in doing business online, if there is a harmonised international standard (a well-drafted international regulation) which promotes core legal principles of party autonomy, technological-neutral, confidentiality and security, and implements fair and appropriate procedures.

Overall this book takes a 'solutions to obstacles' approach and evaluates various contemporary key legal issues of electronic commercial transactions

by comparing current legislative frameworks in China, the EU, the US and international organisations. In response to continuous challenges to the legal certainty of online commercial activities due to the rapid development of information technologies, this second edition of the book continues and expands the author's classical debate over the eight 'obstacles encountered in electronic commercial transactions, and gives answers to those obstacles in a clear, yet concise language'.[3] The eight main legal obstacles to electronic commercial transactions are as follows:

1. The determination of the effectiveness of offer and acceptance and the valid incorporation of terms and conditions in electronic contracts.
2. The legal barriers on errors in electronic communications and the battle of forms.
3. The recognition of the effectiveness of electronic signatures, authentication and foreign certificates.
4. The appropriate legal and technical measures for the protection of personal data privacy rights concerning online commercial activities.
5. The establishment of the balance of rights among different rights holders and the fairness to the liability of Internet service providers.
6. The determination of jurisdiction and applicable law concerning Internet-related disputes.
7. The determination of the validity of online dispute resolution agreements and the enforcement of online settlements.
8. The infrastructural building of trusted e-commerce platforms integrated with appropriate organisational, technical and legal measures.

1.2 Key concepts and features

1.2.1 Internet

The Internet, a base of connection for international electronic commerce, is a form of networks connected 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 communications between parties over long distances.

Internet technology first began in the 1960s, and the first transatlantic computer networks were linked up in the early 1970s.[4] Between the 1960s and the early 1990s, the Internet was developed mainly for military, governmental and academic use. Beginning with the late 1990s, when Microsoft released Windows 98 marking the full-scale entry of the Internet browser

3 P. Evans (2011) 'Publication review: law of electronic commercial transactions: contemporary issues in the EU, US and China', *Communications Law*, 16 (1): 41.

4 *An Atlas of Cyberspaces: Historical Maps of Computer Networks.* Available at: http://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/historical.html (last accessed 30 June 2013).

and server, the Internet started to become truly popular for commercial use. In the 2000s, the Internet experienced enormous growth and more and more businesses set up websites to display product information and provide trading platforms for goods and services, while a large number of individuals began to use e-mail and instant messaging as well as shopping online. In the last ten years, businesses have been conducting their activities increasingly over the Internet, including international trade and domestic sales. Most recently, the Internet has been employed in various new industries known as technical-based services, for example, social networking, online banking, digital doorkeys[5] and online dispute resolutions. There are also new emerging technologies relying on networks such as service-oriented computing, beaming technology (virtual reality) and cloud computing.

1.2.2 Electronic commerce

The phrase of 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'.[6] The Organisation for Economic Cooperation and Development (OECD) defines electronic commerce from an economic and social point of view as:

> All forms of commercial transactions involving both organizations 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.[7]

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.[8]

5 'Digital doorkeys and more: meet New York's latest start-ups', BBC News, 3 May 2013. Available at: http://www.bbc.co.uk/news/business-22372102 (last accessed 30 June 2013).

6 European Commission, Working Paper, *eEurope, an Information Society for All.* Available at: http://europa.eu/legislation_summaries/information_society/strategies/l24221_en.htm (last accessed 30 June 2013).

7 *Electronic Commerce: Opportunities and Challenges for Government* (1997), at p. 11.

8 *A European Initiative in Electronic Commerce*, COM (1997) 157 final of 16.4.1997, at I (7).

The key words of the above definition 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,[9] trade[10] and business[11] for both non-personal and personal usage. There are also 'indirect electronic commerce' (electronic ordering of tangible goods) and 'direct electronic commerce' (online delivery of intangibles).[12]

Electronic commercial transactions are one of the main components of electronic commerce and 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 mainly two 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.[13] 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 for B2C electronic commerce is electronic retailing.

In general, B2B provides 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 most countries' GDP (gross domestic product).

1.2.3 Service-oriented computing and cloud computing[14]

In recent years new technologies have been continuously emerging and some of these have been deployed to facilitate efficient electronic commercial transactions. Service-oriented computing and cloud computing are the

9 'Commerce: the activities involved in buying and selling things' (*Cambridge Advanced Learner's Dictionary*).

10 'Trade: the activity of buying and selling, or exchanging, goods and/or services between people or countries' (*Cambridge Advanced Learner's Dictionary*).

11 '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*).

12 *A European Initiative in Electronic Commerce*, COM (1997) 157 final of 16.4.1997, p. 4.

13 N. Rosner (2004) 'International jurisdiction in European Union e-commerce contracts', in N.S. Kinsella and A.F. Simpson (ed.), *Online Contract Formation* (New York: Oceana Publications), p. 483. An example of performance against performance is when one party supplies statistical data in exchange for the results of market research.

14 Part of this section draws upon the author's other publications: F. Wang and N. Griffiths (2010) 'Protecting privacy in automated transaction systems: a legal and technological perspective in the EU', *International Review of Law, Computers and Technology*, 24 (2): 153–62, and F. Wang (2013) 'Jurisdiction and cloud computing: further challenges to Internet jurisdiction', *European Business Law Review* 24 (5): 589–616.

most commonly adopted in industry and business, though other technologies such as beaming technology[15] and Google Glass[16] may soon be employed for commercial use.

Recent widespread growth in the number and complexity of distributed systems in dynamic business environments has led to the creation of sophisticated tools and technologies to support the design, development and management of automated transaction systems that are integrated with data and privacy protection. Two automated computing technologies in particular, namely agent-based systems and service-oriented computing, stand out as being able to support the required autonomy, flexibility and proactive and reactive characteristics in dynamic business environments. At the same time, agent-based systems and service-oriented computing can generate a secure system that provides the protection of personal data and privacy. Agent-based systems can establish and adopt certain personal data and privacy protection rules, while service-oriented computing offers a promising solution in discovering other appropriate agents, reaching agreements between service providers and customers, managing the joint execution of tasks, and dealing with any problems that arise. Service-oriented computing (SOC), also known as service-oriented architectures (SOAs), is a paradigm for distributed system development that allows software developers to focus on the fulfilment of the required enterprise functionalities at a conceptual level through the provision of standardised communication protocols, interfaces, workflows and service management infrastructures. SOC allows developers to build the functionality that they require by combining existing components, called services, without being concerned by the barriers of heterogeneous operating systems, hardware environments, development platforms or geographical location.

Although the notion of SOAs is backed by numerous organisations, a number of varying definitions have been proposed by a selection of industry bodies, researchers and standards organisations. W3C defines a service as an abstract resource that represents a capability of performing tasks, reflecting on a coherent functionality from the point of view of provider entities and requester entities.[17] The key point in this definition is that a service provider is able to package specific functionality in a suitable format for consumption by a requester. IBM defines SOAs as 'an approach to build distributed systems that deliver application functionality as services to end-user applications or to build other services. SOA can be based on web services, but it

15 Beaming is 'the process of instantaneously transporting people (visitors) from one physical place in the world to another (the destination) so that they can interact with the local people there'. Available at: http://beaming-eu.org/the_project (last accessed 30 June 2013).

16 Introduction to Google Glass. Available at: http://www.google.com/glass/start/ (last accessed 30 June 2013).

17 D. Booth, H. Haas, F. McCabe, E. Newcomer, M. Champion, C. Ferris and D. Orchard (2005) *Web Services Architecture.* Available at: http://www.w3.org/TR/ws-arch/ (last accessed 30 June 2013).

may use other technologies instead.'[18] Web services are one of the more popular technologies that are used to implement SOAs, having received wide industrial support. Services can be primitive or can be built from other services through a process called composition. An important feature of composition is that the component services may be supplied by different providers. This aspect is captured by the definition used by the OASIS consortium, which defines SOAs as 'a paradigm for organising and utilising distributed capabilities that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with and use capabilities to produce desired effects consistent with measurable preconditions and expectations.'[19] A set of standards and metrics are therefore required for SOAs so that services can be provided, consumed and evaluated in a consistent manner. Several alternative standards have been proposed for the various aspects of SOAs, and although the technical details may differ between specific standards, the overall functionalities and characteristics defined are broadly similar.

The combination of agent-based systems and service-oriented computing allows complex business processes to be defined and automatically managed by autonomous agents that can select appropriate services and even reconfigure business processes at run-time according to user preferences and QoS criteria. It is known that in any service-oriented interaction, issues such as the effectiveness of automated contracts and the protection of data privacy still need to be addressed to ensure that an automated agreement is enforceable and all parties are appropriately protected in an agreement that also defines the non-functional commitments that each party should make.

Parallel to other technological developments, cloud computing has also been deployed by businesses and individuals. Cloud computing can be defined as follows:

> a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[20]

18 M. Colan (2004) 'Service-oriented architecture expands the vision of Web services, Part 1'. Available at: http://www.ibm.com/developerworks/webservices/library/ws-soaintro.html (last accessed 30 June 2013).

19 OASIS (2008) OASIS Reference Architecture for SOA Foundation, Version 1.0, OASIS Public Review Draft 1. Available at: http://docs.oasis-open.org/soa-rm/soa-ra/v1.0/soa-ra-pr-01.pdf (last accessed 30 June 2013).

20 The National Institute of Standards and Technology (NIST) Definition of Cloud Computing, US Department of Commerce, Special Publication SP800-145, September 2011. Available at: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (last accessed 30 June 2013), p. 2.

In brief, it can be understood as 'access to computing resources (storage, processing and software), on demand, via a network'.[21] This definition highlights the characteristics and benefits of cloud computing. That is, cloud computing is a model of a computing design and global infrastructure that is available and accessible anywhere for remote storage and processing of data. This type of technological innovation and optimisation may change the way we work, communicate with each other and share information, because access to computing resources has shifted from an internal network to a public network, in particular in the public cloud environment. There are also new participants in such a new environment which as a result may challenge the allocation of responsibility among cloud providers, cloud customers and cloud users. Subsequently it may also affect the attribution of title to data controllers and data processors. National and regional governments have been working on nationwide strategies on the deployment of cloud computing.

In the US the Federal Cloud Computing Strategy was issued on 8 February 2011.[22] It is designed to: 'articulate the benefits, considerations, and trade-offs of cloud computing; provide a decision framework and case examples to support agencies in migrating towards cloud computing; highlight cloud computing implementation resources; identify Federal Government activities and roles and responsibilities for catalysing cloud adoption'.[23]

In the EU it was anticipated that the European Commission would publish a strategy on stimulating cloud computing in Europe in 2012.[24] Developing an EU-wide strategy on cloud computing notably for government and science was one of the eight action plans in the European Commission's Digital Agenda for Europe in 2010.[25] Subsequently, the Digital

21 Guidance on the Use of Cloud Computing, UK Information Commissioner's Office, 20121002 Version 1.1, October 2012. Available at: http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/online/~/media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx (last visited on 30 June 2013), p. 1.

22 The Federal Cloud Computing Strategy, 8 February 2011, The White House, Washington, DC. Available at: http://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf (last visited on 30 June 2013).

23 The Federal Cloud Computing Strategy, 8 February 2011, The White House, Washington, DC, p. 2.

24 Digital Agenda for Europe: Annual Progress Report 2011, 22 December 2011, Brussels. Available at: http://ec.europa.eu/information_society/digital-agenda/documents/dae_annual_report_2011.pdf (last accessed 1 February 2013), p. 3.

25 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe, Brussels, 26.8.2010, COM (2010) 245 final/2. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF (last accessed 30 June 2013), pp. 23–4.

Agenda Annual Progress Report (hereinafter 'the 2011 Annual Progress Report') was issued on 22 December 2011. The 2011 Annual Progress Report has identified eight pillars of work in progress and emphasised that the purpose of launching an overall strategy on cloud computing is to provide 'a better offer of high-speed Internet and better communication infrastructure for more citizens'.[26] In 2011 there was also a public consultation on cloud computing in Europe conducted by the Commission. The public consultation was conducted between 16 May 2011 and 31 August 2011 and the Public Consultation Report on Cloud Computing was released on 5 December 2011.[27]

In China, the Special Regulatory concerning China Cloud in response to the Twelfth Five-Year Plan in Chinese Economy (hereafter 'the China Cloud Computing Consultation') was released by the Ministry of Science and Technology of the People's Republic of China in June 2012.[28] In general, this Consultation specified three main aims for the technological development of cloud computing in China: (a) standardisation of cloud computing services; (b) ensuring the optimisation of cloud delivery and consumption systematic models through technological innovation; and (c) the implementation of such models in industries and government organisations.[29] It also recognised the existing challenges to reach the goals such as the lack of macro management strategies, standardised security measures and regulations on data privacy protection in cloud computing. In order to remove the obstacles, sound strategic measures need to be in place. Such measures, as proposed in the China Cloud Computing Consultation, should include: the implementation of national-level cloud computing strategies consistently at local and department levels; the enhancement of financing support; the encouragement of technological innovation; the training of specialists; the development of international dialogues and collaboration; and the improvement of the regulatory framework for cloud computing.[30]

Among countries there is a general consensus that in order to benefit the employment of cloud computing in industry and daily life, not only is a well-balanced country-level or region-level strategy on cloud computing needed,

26 Communication on e-commerce – frequently asked questions. Reference: MEMO/12/5, 11/01/2012, Brussels, 3.

27 Cloud Computing: Public Consultation Report, European Commission, Brussels, 5 December 2011. Available at: http://ec.europa.eu/information_society/activities/cloudcomputing/docs/ccconsultationfinalreport.pdf (last accessed 30 June 2013).

28 Consultation on China Cloud Computing Development: The Special Regulatory in response to the Twelfth Five-Year Plan in Chinese Economy, the Ministry of Science and Technology of the People's Republic of China, June 2012. Available at: http://www.most.gov.cn/tztg/201206/W020120621537448430735.pdf (last accessed 30 June 2013).

29 Ibid., pp. 4–6.

30 Ibid., pp. 8–10.

but what also is required is the consistent application and implementation of such strategy that meets the international standards.

1.3 Benefits: economic and social impacts

The advent of electronic commerce has been beneficial to the global economy and social society. It is an innovation in the way of doing business that changes the habit of business entities and individuals gradually and to a large degree. 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 to buy and sell online. Buyers can surf the websites, choose the products they want and make payments over the web. 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. For intangible goods, delivery will be executed online. The profound impact of electronic commerce in the global economy and modern society lies in a shortening of the distance between seller and buyer and a simplification of the process of shopping or trading. Such an e-trading system will undoubtedly improve economic efficiency, competitiveness and profitability.

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

- increase internal organisational and management efficiency;
- increase transaction efficiency and reduce transaction costs for both suppliers and buyers;
- extend market reach of suppliers and increase choice for both suppliers and consumers;
- provide accurate information to improve service delivery such as in health provision or the provision of information to consumers.[31]

Most of the expected benefits above have become a reality during the last 15 years. In the Ministerial Meeting of the OECD, a Statistic Profile was updated in June 2011 foreseeing the future of the Internet economy.[32] The statistics show that the Internet has changed the traditional behaviour of businesses and consumers and opened up new market opportunities, although

31 *A Global Action Plan for Electronic Commerce, Prepared by Business with Recommendations for Governments*, ICC, 2nd edn, October 1999. Available at: http://www.iccwbo.org/policy/ebitt/id2422/index.html (last accessed 30 June 2013).

32 *The Future of the Internet Economy: A Statistical Profile*, Organisation for Economic Cooperation and Development (OECD), June 2011 Update. Available at: http://www.oecd.org/sti/ieconomy/48255770.pdf (last accessed 30 June 2013).

concerns about security, trust and privacy are still preventing a large number of Internet users from buying online. For example:

- In 2011 there were 327 million fixed Internet subscriptions in OECD countries, equivalent to 27 per cent of the total population. This number has doubled over the past ten years.
- There were about 733 million registered Internet hosts worldwide in 2010, 17 times more than in 1999.
- Around 30 per cent of people in the OECD buy goods or services over the Internet. Over half do so in the United Kingdom, Denmark, Norway, Korea, the Netherlands and Australia.
- In the EU, 35 per cent of Internet users do not buy online because of security concerns. More than 60 per cent still prefer to go to physical shops out of loyalty or to see the products in person.[33]

China, a non-OECD country, has also had a significant increase of Internet users in recent years according to the Statistical Report on Internet Development in China (January 2013).[34] It is estimated that by the end of December 2012 China had a total of 242 million online shoppers, and the utilisation ratio of online shopping rose to 42.9 per cent, while mobile phone Internet users hit 420 million, growing at the annual rate of 18.1 pr cent in China.[35]

The statistics above prove that electronic commerce has been developing rapidly and has now become a dominant form of commercial activity. The variety of Internet connection devices and available services has also been expanding. This provides companies, in particular small and medium-sized enterprises (SMEs), with lower market entry costs and the ability or possibility to extend their geographic reach to a much larger market. It moves the 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 an important role in modern society to improve commercial connections between enterprises and individuals at national, regional and global levels, to stimulate the internationalisation and globalisation of the economy and production by creating opportunities for the free movement of goods, services, money, people, technology, information and communication, and to generate new challenges for potential market growth in the future.

33 Ibid.

34 The 31st Survey Statistical Report on Internet Development in China, China Internet Network Information Centre (CNNIC), January 2013. Available at: http://www1.cnnic.cn/IDR/ (last accessed 30 June 2013).

35 Ibid., p. 5.

International regulatory harmonisation for a global electronic commercial market will be crucial to the free flow of information and the safety of electronic commercial transactions and other Internet-related commercial activities. In addition, a consistent global standard of the law of electronic commercial transactions will be one of the fundamental elements in the building of users' trust and confidence in conducting cross-border business and sharing information online.

1.4 Legal background to the rise of electronic commercial transactions

1.4.1 Contracts for the sale of goods and provision of services: B2B and B2C

As discussed earlier there are two main forms of electronic commercial transactions: B2B and B2C. Both may share the same formality, although international B2B commercial transactions may be subject to international trade regulations and other forms of legal documents (such as contracts of carriage of goods – bills of lading) and B2C commercial transactions may be subject to consumer protection regulations at national and regional levels. In B2C electronic commercial transactions, it is most common that consumers pay the product fees online using their credit or debit cards. In B2B electronic trading transactions, electronic letters of credit (known as 'electronic documentary credit') are the most popular method to pay goods against bills of lading.

The traditional way of doing international trade starts when the buyer visits a trade fair or the seller's company or factory. Then the buyer will select a product, ask for a quotation for the price and consult about packaging, date and methods of delivery of the goods, as well as payment. If the price quotation for the international sale of goods includes the price of the goods themselves and all the fees up to the transfer of the goods for shipment, then this is known as a FOB (Free on Board) contract. Sometimes the price quotation will not only include the FOB price but also the fees for freight and insurance. The seller is also required to prepare transport and insurance documents, which shall be transferred to the buyer. This 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*.[36]

With the adoption of information technology, nowadays, buyers 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

36 *Arnhold Karberg & Co.* v. *Blythe Green Jourdain & Co.* [1916] 1 KB 495, CA.

contract either online or offline, the parties shall insert a choice of law clause stating by which country's law the contract will be governed. 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 International Chamber of Commerce (ICC) standard trade terms Incoterms 2010[37] 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 UNCITRAL, they might choose CISG as the applicable law. Currently, two-thirds of countries in the world involved in international trade, are contracting parties to the CISG 1980. Both China and the US ratified the CISG, thus in the absence of an effective applicable law clause, its 'default rules' on contract formation and performance will govern contracts for the 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 United Nations Convention on the Use of Electronic Communications in International Contracts (hereafter 'the UN Convention'), adopted in 2005, is deemed to be an international instrument that complements the CISG in the era of the 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 and not to contracts concluded for personal, family or household purposes.[38] The difference is that the CISG only applies to contracts for the international sale of tangible goods where the parties' places of business are in different states and not to service contracts between parties,[39] 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 the sale of goods and services.[40] It is debatable whether contracts for the supply of intangible goods (such as software) should be considered as service contracts, in particular the supply of individualised/custom-made software rather than standardised/ready-made software.

Secondly, with regard to the issue of the validity of electronic communications, the UN Convention performs a supplementary role to the CISG in the legal recognition of electronic communications with regard to forms, because

37 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. More detail is available at: http://www.iccwbo.org/products-and-services/trade-facilitation/incoterms-2010/ (last accessed 30 June 2013).

38 CISG, Article 1, and the UN Convention, Article 2(a).

39 CISG, Articles 1 and 3.

40 The UN Convention 2005, Article 1.

the UN Convention explicitly recognises the legal equivalence of electronic contracts and signatures to written forms.[41] 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, as 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,[42] and suggested that a contract may be concluded or evidenced by electronic communications as the CISG (Article 11) does not 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,[43] while the UN Convention adopts a functionally equivalent and 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 specifies the rules of ascertaining the location of the parties acting over the Internet,[44] while the CISG (Article 10) provides limited rules for determining a party's 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 UN Convention establishes a standard language in determining the time of dispatch and receipt of electronic communications[45], whereas the CISG (Articles 15 and 18(2)) uses a term 'reach' to describe the dispatch and receipt of a message that '(1) an offer becomes effective when it reaches the

41 The UN Convention 2005, Articles 8 and 9.

42 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 accessed 30 June 2013).

43 Ibid.

44 The UN Convention 2005, Articles 6 and 10(3).

45 The UN Convention 2005, Article 10.

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'[46] as well as 'an acceptance of an offer becomes effective at the moment the indication of assent reaches the offeror.'[47] 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;[48] 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 II).

Lastly but not least, importantly, Article 14 of the UN Convention specially regulates input error 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;[49] however, the Advisory Council does not explain its application to the correction or withdrawal of errors in electronic communications, which have been fortunately compensated by the UN Convention to some certain extent.

With regard to B2C contracts of sale, 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. There are differences in that consumers are the weaker parties in B2C commercial transactions that need particularised rules to protect their 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. Special rules equipped for the protection of consumer rights shall include consumer information, liability of inconformity of the goods or service supplied, 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

46 CISG, Article 15.

47 CISG, Article 18(2).

48 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 accessed 30 June 2013).

49 Ibid.

consumer rights. For example, in the UK, the Sale of Goods Act 1979 applies to the 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 the UK consumer's rights according to the general provisions and additional rights of 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. In China, in April 2013 a draft amendment to the China Consumer Rights Law (1994) was published by the Standing Committee of the National People's Congress (NPC), which provides that online shoppers can return goods within seven days after receipt of goods purchased online and online sellers should refund online shoppers within seven days after goods have been returned.[50] At the regional level, on 8 October 2008 the European Commission adopted the proposal for a Directive on Consumer Rights.[51] It is to update and modernise existing consumer rights, which brings them in line with technological change and strengthening provisions in the key problem areas.[52] In October 2011 the EC Directive on Consumer Rights was adopted, which will be effective from 13 June 2014, and simplifies and merges four existing EU consumer-related directives into one set of rules to ensure a high level of consumer protection.[53] This new Directive is compatible with other new regional instruments, for example, the Rome I Regulation.[54] It is specially geared to the needs of the information society. For example, the EC Directive on Consumer Rights (Article 8) designates the formal requirements for distance contracts which revise the EC Distance Selling Directive (Articles 4 and 5). The requirement that 'information is provided on a durable medium' remains the same but the EC Directive on Consumer Rights (Article 8(1)) expands the requirement that information should be made 'available to the consumer in a way appropriate to the means of distance communication used

50 'Draft amendment stresses consumer rights', The National People's Congress of the People's Republic of China, 2 May 2013. Available at: http://www.npc.gov.cn/englishnpc/news/Legislation/2013-05/02/content_1793913.htm (last accessed 30 June 2013), Article 28.

51 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 accessed 30 June 2013).

52 Proposal for a Directive on Consumer Rights, EUROPA, Consumer Affairs. Available at: http://ec.europa.eu/consumers/rights/cons_acquis_en.htm (last accessed 30 June 2013).

53 Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance (hereafter 'EC Directive on Consumer Rights 2011'), OJ L 304, 22.11.2011 pp. 0064–0088.

54 EC Directive on Consumer Rights 2011, Recital (10).

in plain and intelligible language'. Furthermore, the EC Directive on Consumer Rights (Article 9(1)) provides that the consumer shall have a period of 14 days to withdraw using the model withdrawal form from a distance or off-premises contract, without giving any reason and without incurring any costs.[55]

1.4.2 Contracts for the carriage of goods

In traditional B2C commercial transactions, 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 for the sale of goods for personal, family and household purposes. In contrast, in traditional B2B commercial transactions, contracts for the sale of goods are often accompanied by contracts for the carriage of goods. An essential difference between contracts for the sale of goods and contracts for the carriage of goods lies in the terms of liability and documentation. 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.[56] 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'.[57] Thirdly, it is a document of title, because possession of a bill of lading is in many respects equivalent to the possession of goods, although it is symbolic.[58]

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

55 EC Directive on Consumer Rights 2011, Articles 9(1) and 11(1).
56 *Leduc* v. *Ward* [1888] 20 QBD 457.
57 *See* Per Salmon J in *British Imex Industries Ltd* v. *Midland Bank Ltd* [1958] 2 QB 542, at 551.
58 *Sanders Bros* v. *Maclean* [1983] 11 QBD 327.

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 shall be physically delivered or faxed. International trade is now making extensive and increasing use of information technology to facilitate cross-border trade. 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 and can easily be 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.[59] Moreover, a paper-based bill of lading may not be easily kept and protected.

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, in an electronic environment, although the speed and efficiency of bills of lading is improved, there are a number of obstacles to the use of electronic bills, in both technological and legal terms. For example, 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 are making efforts to pave 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; and the UN Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea – the 'Rotterdam Rules' – in 2008. The CMI Rules for Electronic Bills of Lading 1990 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 adopt digital signatures to encrypt and authenticate 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 effectively each successive trader is issued a new document transmitted from the ship. The function of paper-based bills of lading is incorporated into electronically generated documents. However, there are some disadvantages of the CMI rules: there is no provision for the

59 S. Beecher (2006) 'Can the electronic bill of lading go paperless?', *International Lawyer*, 40 (3): 627–48.

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.[60] The UNCITRAL Model Law on Electronic Commerce 1996 not only provides general provisions for 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.[61] With regard to substantial rules, 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. The current legal regime governing the international carriage of goods by sea lacks uniformity and fails adequately to 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. On 11 December 2008 the UN Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea (the 'Rotterdam Rules') was adopted providing a uniform and modern regime for the international carriage of goods by sea.[62] 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. The Rules affirm the effectiveness of electronic communications for transport records (Article 3). Articles 8–10 of the Rotterdam Rules cover the recognition and procedures for the use of 'electronic transport records', while

60 S. Girvin (2007) *Carriage of Goods by Sea* (Oxford: Oxford University Press), pp. 162–3.

61 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 accessed 30 June 2013).

62 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 accessed 30 June 2013).

Articles 35–42 govern the effectiveness of contract particulars in 'transport documents and electronic transport records'. The form requirements of electronic signatures and authentication are set out in Article 9 impliedly and in Article 38 explicitly. The Rotterdam Rules incorporate the term of 'electronic transport records' in general provisions parallel to the term of traditional 'transport documents' throughout the whole conventions, whereas most of the other legislation 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 strongly support the efficient usage of electronic means in the shipping industry.

1.4.3 Online security: electronic signatures and data privacy protection

Traditionally the delivery of goods takes place before or after payment by cash. Electronic payments are often required to finalise electronic commercial transactions. Electronic payments can be understood as paying for goods or services via electronic means rather than by cash. Users often need to submit various important data (such as bank account details and home address) in an electronic payment system. With the rapid development of new technologies, technical and legal measures for online security need to be updated to avoid security compromises in order to build users' trust for electronic commercial transactions. It is notable that the mutual recognition of electronic signatures, electronic identification and authentication plays a vital role in facilitating electronic transactions and in strengthening users' trust in them.[63] Electronic signatures and other electronic trust services are not only used to authenticate the identity of senders and the integrity of documents but also to secure payment, personal data processing and storage in electronic commercial transactions.

In B2C electronic commercial transactions, it is most common that consumers pay the product fees online using their credit 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 to make a payment on the Internet, online merchants will only request the credit or debit card numbers and billing addresses. Credit card numbers are at risk of being stolen or kept by online merchants for unauthorised uses, as are the billing addresses. Although consumers' billing addresses may change, those billing addresses can ordinarily

63 Communication of a coherent framework to build trust in the digital single market for e-commerce and online services, European Commission, Brussels, 11.01.2012, COM (2011) 942 final, p. 9.

be obtained from a public telephone book or Internet database. Security and privacy protection is one of the major concerns of online shopping.

Likewise, there is also concern over the security of using e-trading systems for B2B transactions. In B2B trading contracts, the exporter and the overseas buyer usually agree in the contract of sale that payment shall 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. The issuing bank then arranges with a bank in 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; 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.[64] It can be evidenced by a landmark case *Power Curber International Ltd* v. *National Bank of Kuwait*.[65] 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 that '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, which means that the bank is entitled to reject documents which do not strictly conform to the terms of the credit, is referred to as the doctrine of strict compliance. For example, in the case of *Soproma SpA* v. *Marine & Animal By-Products Corporation*,[66] 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 further an analysis certificate stating that the goods had a minimum content of '70% protein'. The sellers tendered to the advising bank in New York bills of lading which did not bear the mark 'freight prepaid' but, on the contrary, bore the mark 'collect freight'; the analysis certificate showed a protein content of only '67%' minimum; and the goods, although described in the invoice as 'fish full meal',

64 Article 4 and 5 of the UCP 600.
65 [1981] 2 WLR 1233.
66 [1966] 1 Lloyd's Rep. 367.

was described in the bills of lading only as 'fishmeal'. The court decided that the buyers had rightly rejected the documents. It is notable that the Uniform Customs and Practice for Documentary Credits (UCP) is a successful international instrument which standardises banking practice relating to letters of credit, issued by the International Chamber of Commerce (ICC). The first version of the UCP rules was published in 1933, while most recently, 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) has been launched by the ICC as a supplement to the UCP in order to accommodate the presentation of electronic records alone or in combination with paper documents.[67] 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.

There are currently various legislative reviews in progress with regard to the general issues concerning the recognition of technical interoperability of electronic signatures, authentication, certificates and trust services at the national, regional and international levels. For example, UNCITRAL has been working on draft provisions on electronic transferable records since 2011.[68] In the EU, the European Commission has been working on a proposal for a regulation on electronic identification and trust services for electronic transactions in the internal market and the European Commission proposed a Regulation on 'Electronic Identification and Trusted Services for Electronic Transactions in the Internal Market' on 4 June 2012.[69] In China, the Ministry of Commerce of the People's Republic of China also proposed the Regulatory Specifications on the Use of Online Signing Process in Electronic Contracts in 2012, together with the Qualification Standard for Electronic Commerce Enterprises.[70]

Moreover, as discussed earlier, with the continuing development of technology, automated decision-making on behalf of individuals is also under way. Under automated systems, personal data including a long history of an individual's activities, behaviours and habits will be analysed and processed. It is difficult for users to know when, where and how personal data is collected

67 eUCP V1.1, Article 1(a).

68 Draft provisions on electronic transferable records, A/CN.9/WG.IV/WP.122, 4 March 2013.

69 A proposal of the Regulation on 'Electronic Identification and Trusted Services for Electronic Transactions in the Internal Market', European Commission, COM (2012) 238 final.

70 Circular of the Ministry of Commerce of the People's Republic of China, on Soliciting Comments on the Regulations of Online Signing Process of Electronic Contract (Draft); and Circular of the Ministry of Commerce of the People's Republic of China, on Soliciting Comments on Qualification Standard for Electronic Commerce Enterprise (Draft), the Ministry of Commerce, *China Foreign Trade and Economic Cooperation Gazette*, Issue No. 63, October 2012. Available at: http://english.mofcom.gov.cn/article/policyrelease/gazette/201301/20130100015518.shtml (last accessed 30 June 2013).

due to the complexity and rapid changes of technologies. With the deployment of cloud computing, data are often not stored or processed in one particular data centre within the same country. The standard of data protection can be different between countries and yet businesses and individuals fear that data may not be adequately protected in a third country due to different standards in different countries.[71] With the recent invention of Google Glass technology, there is also a growing concern over the 'privacy implications of a device that can be worn by an individual and used to film and record audio of other people'.[72] With the possible future introduction of 'beaming' technology for civilian and commercial uses, a robot can physically represent an individual or legal entity to meet with another party or participate in an activity in another place or country, which again raises significant data privacy issues.[73]

With the ever fast-growing technology, legislation is always one step behind the latest invention of computing network services. This leads to a situation where computer scientists and entrepreneurs try to adjust or improve the application of products in order to comply with the existing law, or legislators try to amend the existing law to be compatible with the new technology in order to protect users' rights and enhance public safety without jeopardising technological innovation and market development. In the US, the Federal Trade Commission recommended a privacy framework for businesses and policymakers in March 2012 to protect consumer privacy in an era of rapid change, and called on companies to act now to implement best practices to protect consumers' private information.[74] In China the Decision on Strengthening Online Information Protection, which has the same legal effect as a law, was adopted by the 94th meeting of the chairman and vice chairpersons of the 11th National People's Congress (NPC) Standing Committee in December 2012 in Beijing.[75] In the EU, the EC e-Privacy Directive was amended by Directive 2009/136/EC which entered into force in May 2011. The EC Directive on Data Protection 1995 has also been under review and on 25 January 2012 the European Commission proposed a comprehensive

71 F. Wang (2012) 'Data protection, jurisdiction and cloud computing: the proposal of the General Data Protection Regulation', *Intellectual Property Forum*, 90: 98–102, at p. 99.

72 Letter addressed to Google regarding Google Glass, a type of wearable computing in the form of glasses, 18.06.2013, Article 29 Working Party Website. Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm (last accessed 30 June 2013).

73 'Real-world beaming: the risk of avatar and robot crime', BBC News, 11 May 2012. Available at: http://www.bbc.co.uk/news/world-europe-17905533 (last accessed 30 June 2013); and see also R. Purdy, Deliverable D7.2: Scoping Report on the Legal Impacts of BEAMING Technologies, EU FP7 Networked Media and 3D Internet – 248620, 20 July 2011.

74 Federal Trade Commission (FTC) Report: Protecting Consumer Privacy in an Era of Rapid Change – Recommendations for Businesses and Policymakers, March 2012. Available at: http://ftc.gov/os/2012/03/120326privacyreport.pdf (last accessed 30 June 2013).

75 'China's legislature adopts online info rules to protect privacy', The National People's Congress of the People's Republic of China, 5 January 2013. Available at: http://www.npc.gov.cn/englishnpc/news/Legislation/2013-01/05/content_1750014.htm (last accessed 30 June 2013).

reform of the data protection rules known as the 'Proposed General Data Protection Regulation 2012'.[76]

1.4.4 Dispute resolution

Resolving cross-border disputes concerning electronic commercial transactions is inevitably more complicated than in a paper-based environment as it involves various connecting factors such as the place of domicile, the place of business and the place of performance that are difficult to determine in the online environment in the absence of choice-of-court and choice-of-law clauses in contracts. Moreover, the determination of Internet jurisdiction and applicable law has been further challenged when online contracting or transactions with the online delivery of intangible goods are executed in several places and it is difficult to ascertain the principal place of performance. Even if there are conflict-of-law clauses in contracts, the determination of the effectiveness of electronic exclusive jurisdiction and applicable law clauses/agreements may also encounter legal challenges due to lack of interpretation in existing laws and the rapid changes of technologies.

It is known that a long-term business relationship is crucial for business maintenance and further development. Forming and keeping an ongoing healthy international business relationship requires businessmen's interpersonal communication and negotiation skills and, more importantly, demands the professionalism and maturity of businessmen in dealing with business disputes. It is recommended to include dispute resolution clauses choosing friendly dispute resolution methods in international contracts.

Going to the courts straight away whenever an international trade dispute arises is not a very wise decision as cross-border litigation takes a long time and involves high litigation fees. 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 forms. Resolving disputes online seems to be a logical way to assess digital evidence and also a way of avoiding cross-border travel. Such method is introduced as online dispute resolution (ODR). By moving traditional offline dispute resolution and litigation online, ODR is the equivalent to eADR and a cybercourt. It has been a new, challenging and much researched issue since the mid-1990s. Its occurrence will boost confidence in doing business online and certainly will be more efficient than offline methods in cases

76 Proposed General Data Protection Regulation 2012, COM (2012) 11 final.

that have an 'international' or 'cross-border' factor. However, there are barriers to 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.

Overall, topics in the law of electronic commercial transactions can be divided into three main pillars: (1) electronic contracts; (2) online protection; and (3) dispute resolution. This book aims to provide in-depth research into finding solutions to remove eight generic legal obstacles to electronic commercial transactions. This research is based on interdisciplinary work on law and technology. Its methodology involves a theoretical approach by conducting comparative and conceptual analysis to evaluate current legal frameworks, and a practical approach by comparing current legal practices and their impacts on industries, businesses and individuals in the EU, US and China. It proposes constructive ways to achieve the modernisation and harmonisation of laws at the national, regional and international levels in response to the rapid development of technology. It shares best practices for legislators, politicians, practitioners, scholars, businesses and individuals and offers insights into policymaking, law reforms, regulatory developments and self-protection awareness.

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 sales 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.

Stage 2

The website has written in bold at the bottom of each page 'For our full terms and conditions please click on this PDF file or hyperlink.' The terms and conditions state that tickets can only be refunded within seven days of delivery. B's computer is old and slow and therefore he does not access the PDF file of terms and conditions but is able to access them via a hyperlink. So B clicks a hyperlink and 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 3

A never knows that this transaction has occurred. The website also does not clearly give B an opportunity to know when the contract is finally concluded. B also cannot download or print a copy of the terms and conditions. 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 4

Only after the conclusion of the contract does B realise that tax is not included in the price and also that the price of the tickets is much higher than originally indicated as it has changed while the buyer was acting on the website. B can only take one piece of hand luggage on the flight and will have to pay additional fees for any check-in luggage. Meanwhile, B also realises that he input the wrong quantity of tickets. Instead of booking for one person, he orders and pays for two.

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

Legal concerns in response to the scenario

- Does the above transaction constitute a valid contract?
- When is the offer effective and when is the acceptance to the offer effective?
- Is B bound by the terms and conditions in the PDF file and/or via a hyperlink?
- Does A have a right to amend the wrong advertisement on the website after the order has been made?
- Is 'error in electronic communications' equivalent to 'the traditional mistake and misrepresentation in contracts'? If not, what are the differences?
- What are the duties and liabilities of Internet service providers?

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

1. What is electronic contracting?
2. Who is contracting?
3. When is an electronic contract made?
4. What are the terms and conditions?
5. 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 the purposes of

contract formation.[1] Neither does the most recent international instrument, the UN Convention on the Use of Electronic Communications in International Contracts (hereafter 'the 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 neither imposes a duty of making electronic contractual terms available in a particular manner nor the legal consequences of its failure. That is, the UN Convention does not intend to affect the application of any rule of law concerning the requirement of a particular manner in which to incorporate terms and conditions, according to Article 13 of the UN Convention.[3] If the law requires that a communication or a contract should be in writing, such requirement is met by electronic communication if the information is accessible for subsequent reference according to Article 9(2) of the UN Convention. In the EU, the EC Directive on Electronic Commerce[4] and the EC Distance Selling Directive (replaced by the EC Directive on Consumer Rights in 2014)[5] set the requirements of accessibility, reproducibility and storability of contract terms and general conditions. In the US, the Uniform Electronic Transactions Act (UETA) requires transferability and accessibility of a record.[6] In China, the Electronic Signature Law also requires the reproducibility of data messages such as terms and conditions.[7] However, there are no such obligations under the UN Convention on Contracts for the International Sale of Goods (CISG) or most of the other

1 J. A. E. Faria (2006) 'The United Nations Convention on the Use of Electronic Communications in International Contracts – an introductory note', *International and Comparative Law Quarterly*, 55 (3): 689–94, at p. 691.

2 The 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 accessed 30 June 2013).

3 UN Convention on the Use of Electronic Communications in International Contracts 2005 (hereafter 'the UN Convention'), Article 13.

4 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 Internal Market ('Directive on Electronic Commerce'), Article 10(3).

5 Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts (hereafter 'EC Distance Selling Directive'), Article 5(1); see also Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance (hereafter 'EC Directive on Consumer Rights 2011'), which takes effect on 13 June 2014, Official Journal L 304, 22/11/2011 P. 0064–0088.

6 US Uniform Electronic Transactions Act (UETA) 1999, Sections 12 and 16.

7 China Electronic Signatures Law, Article 5(1).

international instruments dealing with commercial contracts.[8] 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, while if 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. For example, an act of hyperlinking may result in directing users to access temporary documents/agreements, copyrighted materials or an unauthorised database. It may raise concern on the validity of terms and conditions via a hyperlink on a website for distance selling due to its non-durability for later access or reference.[9]

Thirdly, the UN Convention introduces the use of automated message systems,[10] recognising the possibility of concluding a contract by electronic agents without any human intervention in an automated message system. Automated message systems, also known as 'electronic agents', refer essentially to systems for the automatic negotiation and conclusion of contracts without the involvement of a person, at least at one of the ends of the negotiation chain.[11] That is, 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 one or both parties have interacted in the contracting process by using an automated message system without review by any person, or a contract is formed by the interaction of two automatic message systems.[12] In the US, the UETA also 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'.[13] In the EU, the EC Directive on Electronic Commerce lacks specific rules on that matter, though it generally acknowledges that 'Member States shall ensure that their legal system allows contracts to be concluded by electronic means'.[14] 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.[15] 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

8 Explanatory Note 2007, p. 71.
9 A hyperlink is a URL (Uniform Resource Locator) address or a clickable link which can be embedded in words or images, providing instant access to another page/document in an internal or external site.
10 The UN Convention 2005, Article 12.
11 Explanatory Note 2007, p. 40.
12 The UN Convention 2005, Article 12.
13 UETA 1999, Section 14.
14 The EC Directive on Electronic Commerce 2000, Article 9(1).
15 Explanatory Note 2007, p. 69.

operated.'[16] Although the UN Convention has made a significant recognition of automated message systems, there is a query about whether the rules of automated message systems will 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. This leads to the issue of the validity of incorporating terms and conditions under automated transaction systems.

The next issue which is intertwined with the above issues 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 automated e-contract system, because in the meanwhile it allows time for the amendment of errors. In the EU, the EC Directive on Electronic Commerce also stipulates that the service provider should 'make 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.'[17] In the US, the UETA also provides measures to inform and correct errors in an automated transaction.[18] None of the legislation clarifies the timing and manner of error notification and correction.

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, though the US Uniform Electronic Transactions Act and the UNCITRAL Model on Electronic Commerce have relevant provisions concerning 'time and place of dispatch and receipt of an electronic communication'.[19] The UN Convention has established a provision in an attempt to remove the uncertainty of determining the location of parties. It is debatable whether this provision under the UN Convention is sufficient and practical for the determination of the location of parties. For example, with the further functional development of automated computing systems (such as service-oriented computing) and cloud computing, decision-making regarding

16 Explanatory Note 2007, p. 70.
17 EC Directive on Electronic Commerce 2000, Article 10(1)(c) and Article 11(2).
18 UETA 1999, Section 10.
19 UETA 1999, Section 15, and UNCITRAL Model Law on Electronic Commerce 1996, Article 15.

the sale of goods or services can be done automatically with standard terms and conditions without any human interaction between two international trading companies frequently doing business with each other. The automated systems can design and offer a most favourable sale package to the buyer based on the information that the buyer gives, history of choice preferences and other data sources that the seller collects such as market prices, currency exchange rates and new modules, etc. Once the supply matches the demand (it usually takes a few seconds), an international contract of sale will be automatically concluded by the automated trading systems and digital goods/services will subsequently be provided by electronic means. Although business could benefit from such a system in terms of convenience and efficiency, there is potentially legal uncertainty with regard to the validity of automated electronic agreements and the location of parties in relation to the location of performance of the contract.

Finally, the battle of forms, which is the most complicated issue in commercial contracts, raises barriers to offline contracting. Electronic contracts add an even harder element into this dimension. Whether the existing international and national instruments dealing with the battle of forms are adequate to applying to the battle of electronic standard contracts should be examined.

The solutions to the obstacles in electronic contracting 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. How can terms and conditions be incorporated online?
5. What are the remedies when errors in electronic communications occur?
6. Where is an electronic contract made?
7. How can the electronic battle of forms be dealt with?

2 What is an electronic contract?

2.1 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'.[3] 'Electronic communication' means 'any communication that parties make by means of data messages',[4] 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.[5] This concept gives a broad definition of electronic means of transactions and makes it compatible with a wide range of possibly developing techniques. For example, forming sale of goods or provision of service agreements via service-oriented computing systems can be deemed the process of electronic contracting. Signing cloud computing service agreements online can also be deemed an act of electronic contracting.

1 General Usage for International Digitally Ensured Commerce (GUIDEC) Version II, International Chamber of Commerce (ICC). Available at: http://www.iccwbo.org (last accessed 30 June 2013).

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 accessed 30 June 2013).

3 The US Uniform Electronic Transactions Act (UETA) 1999 and the US Uniform Computer Information Transactions Act (UCITA) 1999.

4 The UN Convention 2005, Article 4(b).

5 C. K. Wei and J. C. Suling (2006) 'United Nations Convention on the Use of Electronic Communications in International Contracts – a new global standard', *Singapore Academy of Law Journal*, 18: 116–202, at p. 136.

2.2 Features: e-mail v. clickwrap v. shrinkwrap

In general, 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 (e-mail). E-mail can be used to make an offer and communicate an acceptance of that offer. The e-mail 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, an Internet Service Provider (ISP), and then forwarded to the offeree's (offeror's) inbox/mailbox. There seems to be a clear consensus about the validity of e-mail communications at the international level. For example, in the US, in the case of *Rosenfeld* v. *Zerneck*, the Supreme Court of New York also recognised that e-mail was a valid form of communications accepting an offer, although the court dismissed plaintiffs' claim due to the failure of the incorporation of the essential terms in the e-mail.[6] In the UK, in the case of *Bernuth Lines Ltd* v. *High Seas Shipping Ltd* ('The Eastern Navigator'), an e-mail is a valid form in which to communicate the acceptance regardless of being treated as a spam mail by the system.[7] In Singapore, in the case of *SM Integrated Transware Pte Ltd* v. *Schenker Singapore (Pte) Ltd*, the Singapore High Court found that there was a concluded lease agreement between the parties by an exchange of e-mail correspondences.[8] In South Africa, in the case of *Jafta* v. *Ezemvelo KZN Wildlife*, the Labour Court of South Africa further concluded that 'an SMS is as effective a mode of communication as an email or a written document'.[9]

Another common method of online contracting using the World Wide Web is known as a webwrap or clickwrap agreement. Normally, the vendor would provide a display of products on his website and indicate the cost of those products. A customer can scroll through the website previewing the items or products on offer, click on an 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.[10] Forming a webwrap agreement is like taking the goods to the cashier in a shop, except that the cashier will be an electronic agent (such as a computer or other electronic device) instead of a person. Contracts or agreements displayed on a website

6 *Rosenfeld* v. *Zerneck*, 4 Misc.3d 193, 776 N.Y.S.2d 458 (Sup. Ct. Kings Co., NY, May 4, 2004).

7 *Bernuth Lines Ltd* v. *High Seas Shipping Ltd ('The Eastern Navigator')* [2005] EWHC 3020.

8 *SM Integrated Transware Pte Ltd* v. *Schenker Singapore (Pte) Ltd* [2005] SGHC 58; see also *Chwee Kin Keong and Others* v. *Digilandmall.com Pte Ltd* [2005] SGCA 2.

9 *Jafta* v. *Ezemvelo KZN Wildlife* (D204/07) [2008] ZALC 84; [2008] 10 BLLR 954 (LC); (2009) 30 ILJ 131 (LC) (1 July 2008). In England, in the case of *North Range Shipping Ltd* v. *Seatrans Shipping Corp.* [2002] 1 WLR 2397, a similar issue was encountered concerning the malfunction (fault) of an e-mail in that an e-mail was sent but did not enter the recipient's mailbox; however, the case was resolved without having to respond to that issue.

10 R. Ong (2004) 'Consumer-based electronic commerce: a comparative analysis of the position in Malaysia and Hongkong', *International Journal of Law and Information Technology*, 12 (101): 103.

requiring a user to click a button to show acceptance are generally non-negotiable, though in theory they should offer the buyer an opportunity to read, view and download them in their entirety before being accepted. The circumstance can raise the issue of what manner of displaying terms and conditions can constitute an informed consent to the buyer and whether there is truly mutual assent by the parties to the terms of the agreement. In practice, most online retailers, such as Amazon, have procedures combining an e-mail notification after a clickwrap action so as to enhance the validity of the clickwrap agreement. For example, when a customer chooses a product, inputs the quantity, selects a delivery method, clicks a hyperlink to 'Conditions of Use/Conditions of Sale' and finally clicks the 'Place the Order' button to make payment to purchase a product from Amazon's online platform, Amazon will send the customer an e-mail confirming receipt of his/her order and containing the details of that order (the 'Order Confirmation E-mail'). The Order Confirmation E-mail, which specifies the selected products, price, delivery address and estimated delivery date with terms and conditions, is acknowledgement that Amazon has received the customer's order, but does not confirm acceptance of the customer's offer to buy the product(s) ordered. Amazon will later send the consumer another e-mail (called the 'Dispatch Confirmation E-mail') which confirms acceptance of the customer's offer and notifies the dispatch of the ordered product with an estimated delivery date. It then concludes the contract of sale for a product ordered by the customer.[11] The deployment of such procedures helps ensure that the customers are given an opportunity to review and revise their orders and print a hard or PDF copy of the terms and conditions.

A third way of forming an electronic contract is by consenting to a 'shrink-wrap' agreement. A shrinkwrap 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 is not available before the conclusion of the contract of sale should be valid and enforceable,[12] though it appears that courts have been inclining more towards the recognition of shrinkwrap terms without prior disclosure such as in the

11 Amazon Conditions of Use & Sale. Available at: https://www.amazon.co.uk/gp/help/customer/display.html?ie=UTF8&nodeId=1040616&pop-up=1# (last accessed 30 June 2013).

12 *Klocek* v. *Gateway, Inc., et al.* 2000 U.S. Dist. Lexis 9896, 104 F. Supp.3d 1332 (D. Kan., June 16, 2000) – the courts held that the shrinkwrap terms and conditions do not create a binding contract. *Brower* v. *Gateway 2000, Inc.*, 676 N.Y.S.2d 569 (New York Supreme Ct. App. Div. [Aug.] 1998) – a shrinkwrap agreement was validly formed.

leading case of *ProCD, Inc.* v. *Zeidenberg*.[13] 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/she pays, the product can be returned to the merchant.[14] However, the UCITA is not widely adopted in the States. In the EU, there is also a tendency for the requirement to disclose terms and conditions prior to the conclusion of any agreement with consumers according to the EC Directive on Electronic Commerce, the EC Distance Selling Directive (replaced by the EC Directive on Consumer Rights in 2014) and the Unfair Commercial Practices Directive. In e-commerce practice, it is advisable that the seller of software products shall make the terms and conditions available for the purchaser to review prior to the placing of the order by displaying them in the terms on the website or providing a hyperlink to the terms that can be downloaded onto a durable medium for later reference. More detail concerning the valid incorporation of terms and conditions will be discussed in the following section.

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 transactions, parties may not have a chance to read the terms and conditions of contracts precisely. There is a need to establish a certain level of trust, which will, in return, build up users' confidence in concluding electronic contracts. It may be possible to introduce a form of 'trustmark' for contracts, so that a provider can have their contracts approved by an independent third party who can then certify that sufficient protection for the customer (and provider) is in place. However, there are two significant limitations with this approach. First, it places a high barrier of entry to individuals wishing to provide services, since they would need to formulate an appropriate contract and have it validated. A potential solution to this would be to use a broker or proxy service that has template contracts that can be adopted (analogous to sellers adopting the privacy statement and practices and the buying and selling policies of sites such as eBay which in turn are certified by organisations such as TRUSTe), but it is unlikely that such template contracts can be made sufficiently broad to be practical and yet detailed enough to provide appropriate protection. Second, and more importantly, such contracts will be inflexible, requiring approval by the independent third party and impossible to be updated rapidly in

13 *ProCD, Inc.* v. *Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996). See also the EU position in the Commission Notice Guidelines on Vertical Restraints which state that 'this may take the form of a "shrink wrap" licence, i.e. a set of conditions included in the package of the hard copy which the end user is deemed to accept by opening the package', Brussels, SEC (2010) 411. Available at: http://ec.europa.eu/competition/antitrust/legislation/guidelines_vertical_en.pdf (last accessed 30 June 2013).

14 Uniform Computer Information Transactions Act (UCITA), Section 209.

response to circumstances at run-time.[15] This will jeopardise the advantage of flexibility in service-oriented computing that contractual terms for services can be selected and configured at run-time according to user preferences and the current situation.

Efforts to remove legal uncertainty in online contracting have been made at the international, regional and national level. At the 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.[16] 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.'[17] In the EU, the EC Directive on Electronic Commerce contains three provisions[18] 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 a requirement.[19] In China, the National People's Congress adopted the new Contract Law which recognised electronic contracting in March 1999.[20] The new China

15 F. Wang and N. Griffiths (2010) 'Protecting privacy in automated transaction systems: a legal and technological perspective in the EU', *International Review of Law, Computers and Technology*, 24 (2): 153–62, at p. 159.

16 The UN Convention 2005, Article 9.

17 UNCITRAL Model Law on Electronic Commerce, Article 11.

18 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), 17.07.2000 *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).

19 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.

20 C. Zhang and L. F. Lei (2005) 'The Chinese approach to electronic transactions legislation', *Computer Law Review and Technology Journal*, 9: 333, at p. 335.

Contract Law[21] implements several changes in contract formation rules. For example, a contract can now be made in any manner.[22] Under the China Contract Law, writings include agreement, letters, telegram, telex, fax, electronic data information and electronic mail.[23]

2.3 The online contracting parties: who is contracting online?

Who, then, are the contracting parties? Are they seller A, buyer B, or buyer A and B's computers? There is no specific provision defining all possible parties to an electronic communication and their attribution under the UN Convention, though there are relevant provisions that may provide some understanding of the parties who are involved with an electronic communication. For example, Article 1 of the UN Convention sets the scope that it applies to 'parties whose places of business are in different states', but 'neither the nationality of the parties nor the civil or commercial character of the parties or of the contract is taken into consideration'. Furthermore, Article 4(1) of the UN Convention provides the definition of 'originator' and 'addressee' of an electronic communication. 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; 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'. It is notable that in the electronic context one of the challenging issues arises when one party claims that it is not responsible for a transaction completed in its name in an electronic format, in particular in the use of robotic devices and the use of electronic signatures as evidence of authorisation.[24] With the advancement of automated transaction systems and digital devices, the circumstance of defining a responsible party can be even more complex. For example, the recent development of a communications technology called 'beaming' allows 'people a real sense of physically being in another location with other people without actually physically travelling'.[25] The logic of such technology is identical to that of service-oriented computing in that the computing system acting as an agent makes a decision or conducts a transaction. The difference is that

21 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.

22 Article 10 of China Contract Law states: 'A contract may be made in a writing, in an oral conversation, as well as in any other form.'

23 China Contract Law, Article 11.

24 M. Winn (2005) *Electronic Commerce*, 2nd edn (New York: Aspen), p. 293.

25 R. Purdy, Deliverable D7.2: Scoping Report on the Legal Impacts of BEAMING Technologies, EU FP7 Networked Media and 3D Internet – 248620, 20 July 2011, pp. 6 and 13.

there is a robot that physically presents as an agent in beaming technology. If a robot embedded with the beaming technology (known as an agent) is involved in the signing of a contract of sale and delivery of goods, will the party that controls the robot or the party that programs this robot be liable for the mistake in the contract when it happens? Thus there is a need to have criteria that can be used to determine and identify the responsible parties to an electronic communication, in particular in automated transaction systems.

In the scenario, 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.[26] The buyer B's computer cannot be regarded as a contracting party but only a device. If the buyer B's computer embedded with service-oriented computing software that acts on behalf of the buyer conducts automated transactions according to the program preferences, such a device may then be considered an agent for a natural or legal person. For a contract to be effective in law, an electronic agent should signal its intention to want to be bound by the contract. So 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 shall include both natural persons and legal entities. The method of identifying contracting parties online is different from the method offline. 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.[27] 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.[28]

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.[29] 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

26 Explanatory Note 2007, p. 51.
27 Explanatory Note 2007, p. 51.
28 Explanatory Note 2007, p. 53.
29 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').

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.[30] 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 of 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.[31]

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, and not just 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 the electronic signature and authentication, which will be discussed in detail in Part III.

In the US, EU and China, there are similar grounds for 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 UETA does not provide a 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.[32] The explanatory note on Section 9 of the UETA provides that 'The section assures that such rules will be applied in the electronic environment. A person's actions include actions taken by human agents of the person, as well

30 T. K. Leng (2006) 'Note and comments: towards uniform electronic contracting law', *Singapore Academy Law Journal*, 18: 234, at p. 237.

31 A/CN.9/527, para. 108.

32 UETA, Section 2 and 14.

as actions taken by an electronic agent, i.e. the tool, of the person.' The Uniform Commercial Code (UCC) also confirms that 'A contract for sale of goods may be made in any manner sufficient to show agreement, including offer and acceptance, conduct by both parties which recognizes the existence of a contract, the interaction of electronic agents, and the interaction of an electronic agent and an individual.'[33] 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.[34] 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 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.[35]

33 Uniform Commercial Code (UCC), Section 2–204(1).
34 China Electronic Signatures Law, Articles 30 and 31.
35 EC Directive on Electronic Commerce, Article 6(b).

3 When is an electronic contract made?

In the scenario, when was the electronic contract concluded? Was it at the time when B completed the required web form, made a payment by debit card, or clicked '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 and the rules relating to offer and acceptance and also error in electronic communications.

3.1 Dispatch and receipt of an electronic communication

3.1.1 Time of dispatch

Different legal systems use various criteria to establish when a contract is formed. The United Nations Commission on International Trade Law (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 most recent e-commerce convention adopted by UNCITRAL – 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] Although it provides some different wording in these provisions from those in UNCITRAL model laws, it is 'not intended to produce a different practical result, but rather [is] aimed at facilitating the operation of the Convention in various legal systems, by aligning the formulation of the relevant rules with general elements commonly used to define dispatch and receipt under domestic law'.[3]

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 Explanatory Note 2007, p. 16.

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', while Article 15(1) of the UNCITRAL Model Law on Electronic Commerce, consistent with the UETA and China Electronic Signatures Law, provides the following definition: 'the time of dispatch of an electronic communication is the time when it *enters an information (processing) system* outside of the control of the originator or of the person who sent the data message on behalf of the originator.'[4] The UETA further provides a more precise explanation of 'an information system', namely that the information system can be somewhere designated or used by the recipient.[5]

The definition of 'dispatch' in the UN Convention as the time when an electronic communication leaves an information system under the control of the originator, as distinct from the time when it enters another information system, was chosen so as to mirror more closely the notion of 'dispatch' in a non-electronic environment.[6] 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.[7] In the EU, the EC Directive on Electronic Commerce, the EC Distance Selling Directive (replaced by the EC Directive on Consumer Rights in 2014) and the EC Directive on Electronic Signatures are all silent on defining 'the time of dispatch' for an electronic communication. With the overall aim of delivering 'sustainable economic and social benefits from a digital single market based on fast and ultra-fast internet and interoperable applications', since 2010 the European Commission has been working on the Digital Agenda for Europe – A Europa 2020 Initiative.[8] In order to further remove barriers to Europe's digital development and enhance trust in electronic transactions, the European Commission adopted the proposal for a Regulation on 'electronic identification and trusted services for electronic transactions in the internal market' on 4 June 2012 (hereafter 'the Proposed Regulation for Electronic Transactions').[9] The Proposed Regulation for Electronic Transactions has introduced the new concepts of 'electronic time stamp' (Section 5) and 'electronic delivery services' (Section 7) concerning the legal effect of data sent or received using an electronic delivery service which is affected by the date of

4 See also UETA, Section 15(3), and China Electronic Signatures Law, Article 11.

5 UETA, Section 15(3).

6 Report of the Working Group on Electronic Commerce (A/CN.9/571), p. 142.

7 C. K. Wei and J. C. Suling (2006) 'United Nations Convention on the Use of Electronic Communications in International Contracts – a new global standard', *Singapore Academy of Law Journal*, 18: 116–202, at p. 137.

8 The Digital Agenda for Europe, COM (2010) 245 of 19.05.2010.

9 Proposal for a Regulation of the European Parliament and of the Council on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market, COM/2012/0238 final – 2012/0146 (COD), Brussels, 04.06.2012 (hereafter 'the Proposed Regulation for Electronic Transactions').

sending, receipt and any change of data indicated by a qualified electronic time stamp.[10] It is asserted that the electronic time stamp should be 'accurately linked to Coordinated Universal Time (UTC) in such a manner as to preclude any possibility of the data being changed undetectably'.[11] The proposed regulatory framework for electronic time stamp and delivery services in the EU would in theory promote the consistency and legal certainty of the time of dispatch and receipt of an electronic communication if appropriate technical measures were adopted.

Applying the rules of the UN Convention 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, the order form leaves the buyer B's sphere of control. If technical measures on electronic time stamp and electronic delivery services are assumed, they may enhance an accurate and consistent record of time of dispatch of the order form regardless of the time differences between different countries and the different setting of time zones in different computing devices.

3.1.2 Time of receipt

As to the time of receipt of an electronic communication, the UN Convention has a similar rule to the UNCITRAL Model Law on Electronic Commerce but with a different wording. It aims at 'achieving an equitable allocation of the risk of loss of electronic communications'.[12] The UN Convention provides the new wording of 'being capable of being retrieved' 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. 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.[13]

That is, the time of receipt of an electronic communication is the time when it becomes capable of being retrieved by the addressee at an electronic

10 Proposed Regulation for Electronic Transactions 2012, Article 35.
11 Proposed Regulation for Electronic Transactions 2012, Article 33(1)(a).
12 Explanatory Note 2007, p. 61.
13 The UN Convention 2005, Article 10(2).

address designated by the addressee. If an electronic communication is sent to a non-designated address, it is deemed to be received only when the addressee becomes aware that the electronic communication has been sent to that address.

This does not intend to create a different effect to other international and domestic laws such as the UNCITRAL Model Law on Electronic Commerce (Article 15(2)), UETA (Section 15(b)) and the China Electronic Signatures Act (Article 11), but to enhance the effectiveness of an electronic communication taking into account the risk of loss by altering the other wording of 'entering an information processing system from which the recipient is able to retrieve the electronic record' and being 'in a form capable of being processed by that system'.

In the EU, the EC Directive on Electronic Commerce, EC Distance Selling Directive (replaced by the EC Directive on Consumer Rights in 2014) and EC Directive on Electronic Signatures fail to provide a specific provision defining the receipt of an electronic communication, though 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.' That is the principle of 'accessibility' in relation to the proof of the receipt of an electronic communications. However, the EC Directive on Electronic Commerce does not further explain what constitutes being 'able to access'.

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,[14] and the word 'usable' is intended to cover both human use and computer processing.[15] 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.[16]

None of the current international, regional and national legislation covers issues such as 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 is of 'capable of being retrieved', when the electronic communication is capable of being retrieved and whether 'capable of being retrieved'

14 Explanatory Note 2007, p. 51.

15 Ibid.

16 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.

is equivalent to 'being able to access'. In the author's opinion, there are three possible considerations in the determination of the time of receipt of an electronic communication as follows:

- Firstly, accessibility should be defined under the designated address. For example, if A sends B an offer at his home e-mail address which is rarely used for business purposes, it may not be deemed received if B designated his official business e-mail address as the sole address for business purposes. Thus, even though the e-mail is accessible at B's home address, it will not constitute receipt of the electronic communication.
- Secondly, retrievability should be distinct from 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.[17]
- Thirdly, receipt of an electronic communication at a non-designated electronic address should fulfil two conditions: retrievability and awareness. That is, 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 other words, there is a need to have a systematic measure that explains the relationship between accessibility, retrievability and awareness. The new system of 'electronic time stamp' (Section 5) and 'electronic delivery services' (Section 7) under the Proposed Regulation for Electronic Transactions in the EU may provide a solution to such matters as confirming the legal effect of data sent or received using an electronic delivery service which is affected by the date of sending, receipt and any change of data indicated by a qualified electronic time stamp.[18] The electronic time stamp and delivery services can also be deemed to provide additional measures to meet the requirement of 'the acknowledgement of receipt of an electronic communication, electronic record or data message'[19] under the UNCITRAL Model Law on Electronic Commerce, the EC Directive on Electronic Commerce and UETA.

17 Explanatory Note 2007, p. 63.

18 Proposed Regulation for Electronic Transactions 2012, Article 35.

19 'Electronic record' means a record created, generated, sent, communicated, received or stored by electronic means under Section 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.

3.2 Offer and acceptance[20]

3.2.1 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 UN 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 the purposes of this provision, '[t]he term "reaches" corresponds to the point in time when an electronic communication has entered the offeree's server.'[21] 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.'[22]

That is, 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 acknowledgment 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

20 The section of offer and acceptance is an updated reprint of the author's journal article: F. Wang (2008) 'E-confidence: offer and acceptance in online contracting', *International Review of Law, Computers and Technology*, 22 (3): 271–8.

21 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 accessed 30 June 2013).

22 Ibid.

validity of offer and acceptance, but stipulates 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 on 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?

The question regarding when a contract has been validly formed online is critical as it concerns the validity of an electronic commercial transaction. An English case, which is famous as a starting point for the law in this area for later reference in other countries, is *Entores* v. *Miles Far East Corp.*[23] 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 or her 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.[24]

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 and Stahlwarenhandelsgesellschaft mbH.*[25] On this basis, regarding e-mails 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 e-mail 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 when 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 e-mail 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.[26] With regard to a web agreement, the contract would be made where the offeror had acknowledged to the offeree

23 *Entores* v. *Miles Far East Corp* [1955] 2 QB 327; [1955] 2 All ER 493.
24 R. Stone (2005) *The Modern Law of Contract*, 6th edn (London: Cavendish), p. 52.
25 *Brinkibon Ltd* v. *Stahag Stahl and Stahlwarenhandelsgesellschaft mbH* [1983] 2 AC 34.
26 R. Stone (2005) *The Modern Law of Contract*, 6th edn (London: Cavendish), p. 55.

that his or her offer was accepted, either by means of a direct response on the website or by a subsequent e-mail, which is called the 'information duty'.

An online contract will not be binding between 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.

The process of contract negotiation and the formality of forming a contract over the Internet is the same as that in physical reality: invitation to treat, offer and counter-offer, acceptance, consideration and intention to create legal relations. The differences are the speed, devices and methods of processing in the online environment.

The distinction between an invitation to treat and an offer is that an invitation to treat is not binding while an offer, met with acceptance, may form a contractual agreement. A promise with consideration is deemed to bind the parties when an offer is accepted.[27] Although the UN Convention is silent on the validity of offer and acceptance, it provides a definition of 'invitation to make offer'.[28] 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. The rationale of an electronic invitation to treat is identical to that of a traditional paper-based contract. Displaying information on products including price, quantity and delivery method is an invitation to make an 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 a leading English case *Pharmaceutical Society of GB* v. *Boots Cash Chemists*.[29] 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. Thus, in order to identify an offer, the court may look for different ingredients before it will find an offer that is then capable of acceptance. The ingredients of an offer, which may be in writing, by words, conduct and other electronic means, may include:

- a clear display of contractual intent;
- on terms that are fixed;
- on terms that are certain;

27 J. Savirimuthu (2005) 'Online contract formation: taking technological infrastructure seriously', *University of Ottawa Law and Technology Journal*, 2: 105–43, at p. 115.

28 The UN Convention 2005, Article 11.

29 *Pharmaceutical Society of GB* v. *Boots Cash Chemists* [1953] 1 QB 401 (CA).

- on terms that once accepted automatically bind both parties to their agreement.

In the online environment, some websites may try to induce a customer to enter a contract by using misleading statements of terms. 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.[30] The difficulty that may arise in this context is how to strike a balance between a trader's possible intention (or lack thereof) of being bound by an offer on the one hand, and the protection of relying on parties acting in good faith on the other.[31] 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.[32] 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.[33] 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.[34] In addition, terms and conditions should be made available to the other parties online in a particular manner, although the UN Convention is not intended to create special rules for contract formation in electronic commerce.[35] But what will happen if the buyer orders a large quantity of goods that the seller may not be able to supply?

In the traditional common law system, there is evidence of the protection of sellers. For example, in the case of *Grainger & Son* v. *Gough*,[36] 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*.[37] 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 validity of the offer subject to stock availability or detail the estimated quantity of products that are available for sale on the website

30 C. Gringras (2003) *Laws of the Internet*, 2nd edn (London: Butterworths), p. 24.
31 Explanatory Note 2007, p. 66.
32 The UN Convention 2005, Article 11.
33 Explanatory Note 2007, p. 67.
34 Ibid., p. 68. See also the case of *Rosenfeld* v. *Zerneck* (4 Misc.3d 193, 776 N.Y.S.2d 458 (Sup. Ct. Kings Cty. 2004)): the Supreme Court of New York dismissed the plaintiffs' claim due to the failure of the incorporation of the essential terms in the e-mail.
35 UN Convention, Article 13.
36 *Grainger & Son* v. *Gough* [1896] AC 325 (HL).
37 *Esso Petroleum Ltd.* v. *Customs and Excise Commissioners* [1976] 1 WLR 1 (HL).

whereas, in the international e-trade industry, the companies or manufacturers may clarify the possible length of production per unit or container shipment.

3.2.2 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'.[38] 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'.[39] The Proposed Regulation for Electronic Transactions 2012 also does not apply to 'aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form prescribed by national or Union law',[40] though this Regulation may provide a company with the opportunity to 'sign contracts electronically with a counterpart based in a different Member State without fearing different legal requirements for trust services such as electronic seals, electronic documents or time stamping'.[41] Such proposed measures may increase the certainty of the timing of the dispatch and receipt of an offer and acceptance and ensure the integrity and fairness of an electronic record/message for the conclusion of the contract.

Another European contract law instrument for this reference is the Principles of European Contract Law (PECL), which is known as a 'soft law' and not a legally enforceable regulation. It provides a set of model rules and recommends best practices of contract law for Member States. The PECL (Articles 2:205(1) and (2) and 2:206(1) and (2)) stands in the same position as the CISG (Article 18(2)), establishing the acceptance rules to the effectiveness of a contract, which state 'in order to be effective, acceptance of an offer must reach the offeror within the time fixed by it or within a reasonable time.'[42] In contrast to the PCEL, the CISG is a 'hard law' but is only applicable to B2B international commercial contracts. Most of the Member States are contracting parties to the CISG but to date the United Kingdom has not implemented the CISG. In addition, the PECL does not specify special rules for oral offers (as provided in Article 18(2) of the CISG). The rules for oral offers may be helpful because oral offers share the similar characteristics of 'instantaneousness' to clickwrap/web agreements.

In order to further remove legal obstacles to cross-border B2B and B2C business transactions and promote harmonisation in contract law in the Member States, in 2011 the European Commission proposed a Common

38 EC Directive on Electronic Commerce, Article 11(1)(a).
39 EC Directive on Electronic Commerce, Article 11(3).
40 Proposed Regulation for Electronic Transactions 2012, Article 2.
41 COM (2012) 238 final, p. 4.
42 Principles of European Contract Law 2002, Articles 2:205 and 2:206.

European Sales Law (hereafter 'the Proposed Common European Sales Law').[43] One of the main objectives of the Proposed Common European Sales Law is to help traders avoid incurring 'further contract law related costs which stem from the need to adapt the business's website to the legal requirements of each Member State where they direct their activity' in both B2B and B2C e-commerce transactions.[44] Although the Common European Sales Law is an optional instrument, once it is adopted by a Member State it becomes a hard law (a legally enforceable regulation). Some nations such as the United Kingdom are sceptical over such a uniform contract law instrument. It was suggested that certain English doctrines, such as non-recognition/non-requirement of good faith in the context of pre-contractual negotiations in English contract law are considered a virtue so that a uniform contract law including the principle of good faith will just not work in England.[45] In addition, in English contract law the postal rule provides an exception to the acceptance rules on the effectiveness of the acceptance, whereas a uniform law may impose a single and rigid rule that diminishes the benefits of the flexibility of applying the postal rule to the slow mode of communications between two distant places.[46]

Nevertheless, some provisions in the Proposed European Common Sales Law may be helpful to promote harmonisation of the legal certainty for B2B and B2C electronic commercial transactions. For example, the Proposed Common European Sales Law (Articles 35 and 36) provides the acceptance rules on the effectiveness of an agreement: 'where an acceptance is sent by the offeree the contract is concluded when the acceptance reaches the offeror';[47] and 'an acceptance of an offer is effective only if it reaches the offeror within any time limit stipulated in the offer by the offeror or within a reasonable time after the offer was made'.[48] Moreover, the Proposed Common European Sales Law (Section 3) provides a special provision for contracts concluded by electronic means which should in theory promote the standardisation of electronic contract practices in the Member States. For example, it requires the trader's acknowledgment of the receipt of an electronic offer or an acceptance by electronic means and without undue delay.[49] An additional requirement – that 'such acknowledgement shall display the content of the offer or of the

43 Proposal for a Regulation of the European Parliament and of the Council on a Common European Sales Law, COM (2011) 635 final, Brussels, 11.10.2011 (hereafter 'the Proposed Common European Sales Law').

44 Proposed European Common Sales Law 2011, p. 2.

45 G. McMeel and H. C. Grigoleit (2013) 'Interpretation of contracts', in G. Dannemann and S. Vogenauer (eds), *The Common European Sales Law in Context: Interactions with English and German Law* (Oxford: Oxford University Press), p. 346.

46 *Henthorn* v. *Fraser* [1982] 2 Ch 27, CA. This court held that the postal rule was reasonable because the offeree's home (Birkenhead) and the offeror's office (Liverpool) were separated by a significant distance.

47 Proposed Common European Sales Law 2011, Article 35(1).

48 Proposed Common European Sales Law 2011, Article 36(1) and (2).

49 Proposed Common European Sales Law 2011, Article 24(5).

acceptance' – was also proposed to be inserted into Article 24(5) of the CESL by the European Parliament on 6 March 2013.[50] This is to ensure consistency in practice, though there is a need to clarify the 'electronic means' of acknowledgment. For instance, the method of acknowledgment in response to the receipt of an offer and acceptance should be in line with the particular method used in the dispatch of an offer and acceptance though the methods of such acknowledgment can be flexible to a certain degree.

3.2.3 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.'[51] It also specifies that, in the case of a computer information transaction, 'a contract is formed when an electronic acceptance is received'.[52] Unfortunately to date the UCITA has not been enacted by most of the states.

Another two relevant pieces of legislation – the UETA and the E-Sign Act – are silent on the appropriate rule for the timing of an acceptance,[53] though the UETA (Section 14) validates transactions formed between parties by the interaction of their electronic agents even if they were not aware of the resulting terms or agreements. It also validates the formation of contracts by interactions between an electronic agent and an individual who voluntarily performs actions with the knowledge or reason to know that they will cause the electronic agent to complete performance. In contrast to the UETA, the E-Sign Act does not address these issues, while it generally validates the use of electronic agents.[54] Furthermore, the time of dispatch and receipt of an electronic communication in the UETA (Section 15) may be of great relevance to the determination of the effectiveness of an offer and acceptance. As discussed earlier, the UETA (Section 15) is consistent with the UN Convention, though with a different wording which 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 a system to which the addressee has access, and that a

50 Draft Report on the proposal for a regulation of the European Parliament and of the Council on a Common European Sales Law (COM (2011)0635 – C7-0329/2011 – 2011/0284(COD)), Committee on Legal Affairs, European Parliament, 6 March 2013, p. 54.

51 UCITA, Section 202(a) (2001). Available at: http://www.law.upenn.edu/bll/ulc/ucita/ucita200.htm (last accessed 30 June 2013).

52 UCITA, Section 203(4) (2001).

53 V. Watnick (2004) 'The electronic formation of contracts and the common law mailbox rules', *Baylor Law Review*, 56 (1): 175–203, at p. 197; Electronic Signatures in Global and National Commerce (E-Sign) Act 2000.

54 The Electronic Signatures in Global and National Commerce Act (E-Sign Act) 2000, Section 101(h).

record is 'received' when it enters a system designated for the receipt of such information in a form capable of being processed. Although the parties may contractually agree to adopt a different determination of the time of dispatch and receipt of an electronic communication, the UETA provides a standard default rule. Again, the E-Sign Act is silent on this issue.

With regard to the formality of an electronic contract, 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.'[55] The UETA also imposes a record requirement rather than a writing requirement. Both the 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.[56] Therefore both the UCITA and UETA broaden the traditional common law writing requirement and clarify the validity and enforceability of certain electronic contracts.

3.2.4 Chinese legislative framework

In China, the China Contract Law (Article 2) provides the following definition of a contract: 'a contract is an agreement between natural persons, legal persons or other organizations with equal standing, for the purpose of establishing, altering, or discharging a relationship of civil rights and obligations.' It covers an agreement concerning commercial and civil transactions other than any personal relationship such as marriage, adoption and guardianship. It further states that parties may conclude their contract by way of offer and acceptance.[57] Unlike the common law system, consideration is not required to affect the establishment and alteration of an agreement in China.[58]

The offer and acceptance rules of the China Contract Law are similar to the rules of the CISG. The China Contract Law (Article 14) defines an offer as 'a party's *manifestation of intention* to enter into a contract with the other party, which shall comply with the following: (i) Its terms are specific and definite; (ii) It indicates that upon acceptance by the offeree, the offeror will be bound thereby', while Article 21 defines an acceptance as 'the offeree's *manifestation of*

55 UCITA, Section 201(a)(1).

56 UCITA, Section 102(a)(55), and UETA Section 2(13).

57 China Contract Law, Article 13.

58 N. Kornet (2010) 'Contracting in China: comparative observations on freedom of contract, contract formation, battle of forms and standard form contracts', *Electronic Journal of Comparative Law*, 14 (1). Available at: http://www.ejcl.org/141/art141-1.pdf (last accessed 30 June 2013), p. 14.

intention to assent to an offer'. It is inevitable that parties' intention to create legal relations should be shown in order to form a valid agreement in the Chinese contract law system. The parties shall abide by the principle of 'good faith' in exercising their genuine intention to alter, accept or reject an offer in the China Contract Law.[59]

In addition, the common-law postal rule does not apply under the China Contract Law. The China Contract Law employs the acceptance rule with regard to the effectiveness of an acceptance to the offer. 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.[60] If there is no fixed time in the offer, the offer is deemed to be effective within a reasonable time that the offeror should receive the acceptance. According to Article 25 of the China Contract Law, a contract is formed once the acceptance becomes effective. The China Contract Law is flexible in terms of the method of the acceptance, which can be either by notification or 'by conduct in accordance with the relevant usage or as indicated in the offer'.[61] In the case of *Guangzhou Maritime Rescue and Salvage Bureau* v. *Fuzhou Xiongsheng Shipping and Trade Co., Ltd*, it was held that a maritime rescue contract was effectively accepted by the plaintiff's sending a rescue ship to the defendant's stranded ship in response to the defendant's request.[62] If the acceptance is communicated by electronic means, either the time when the electronic message enters into a designated specific system is deemed its time of arrival, or the time when the electronic message first enters into any of the recipient's systems (without a designated specific system) is deemed its time of arrival.[63] The contract is formed upon the execution of the confirmation letter if parties enter into a contract by the exchange of letters or electronic messages and require the execution of a confirmation letter before the contract is formed.[64]

In contrast to the China Contract Law, the China Electronic Signatures Law does not directly regulate the rules of offer and acceptance of electronic contracts. Instead, the China Electronic Signatures Law (Articles 9 to 12) further deals with the sending and receipt of data messages, which are consistent with the China Contract Law and identical to relevant provisions in the UETA and the UN Convention. Article 10 of the China Electronic Signatures Law 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

59 China Contract Law, Article 6.
60 China Contract Law, Article 23.
61 China Contract Law, Article 22.
62 *Guangzhou Maritime Rescue and Salvage Bureau* v. *Fuzhou Xiongsheng Shipping and Trade Co., Ltd re a Maritime Rescue Contract*, PRC Maritime Ct, 27 March 2001.
63 China Contract Law, Articles 16 and 26.
64 China Contract Law, Article 33.

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 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 recipient for the first time shall be regarded as the time for receiving the data message.

In order to further regulate online contracting behaviour in a variety of e-commerce transactions and protect the legitimate rights and interests of enterprises, the Ministry of Commerce of the People's Republic of China proposed the Regulatory Specifications on the Use of Online Signing Process in Electronic Contracts in 2012 (hereafter 'China Specifications for Electronic Contracts (Draft)'), together with the Qualification Standard for Electronic Commerce Enterprises.[65] The China Specifications for Electronic Contracts (Draft) complement the China Electronic Signatures Law and provide the definition of 'electronic contract', 'the signing system of electronic contract', 'the third-party storage service provider for electronic contracts' and 'the service provider of electronic signature and certificate authentication'.[66] The Specifications also specify three key principles to create a fair e-commerce environment, namely 'confidentiality', 'an independent and separate system for backup storage' and 'security' in e-commerce transactions.[67] It appears that one of the key features of the Specifications is to emphasise the importance of technical back-up measures during the process of the online contract negotiation in case of technical failure or interruption, which may affect the effectiveness of an offer and acceptance and the integrity of data messages. There are no substantive rules regulating the formality of an electronic offer and acceptance in the Specifications.

3.2.5 Can the postal rule apply to e-contracting?

After reviewing the current contract law legislation in the EU, US and China, it is notable that there are mainly two rules regarding the effectiveness of an acceptance: namely, the postal rule and the acceptance rule. The postal rule only applies to an acceptance, and not to any other type of communication

65 Circular of the Ministry of Commerce of the People's Republic of China, on Soliciting Comments on the Regulations of Online Signing Process of Electronic Contract (Draft), and Circular of the Ministry of Commerce of the People's Republic of China, on Soliciting Comments on Qualification Standard for Electronic Commerce Enterprise (Draft), the Ministry of Commerce, *China Foreign Trade and Economic Cooperation Gazette*, Issue No. 63, October 2012. available at: http://english.mofcom.gov.cn/article/policyrelease/gazette/201301/20130100015518.shtml (last accessed 30 June 2013). 《电子合同在线订立流程规范》(征求意见稿) and 《电子商务企业资质认定标准》(征求意见稿).

66 China Specifications for Electronic Contracts (Draft) 2012, Article 3.

67 China Specifications for Electronic Contracts (Draft) 2012, Article 4.

such as an offer or a counter-offer.[68] Communication of the offer is required in virtually all situations as the person to whom the offer is addressed must be aware of it.[69] Subsequently the question concerns the prevailing rule to determine the effectiveness of an electronic acceptance. An answer may be sought from social, historical, economic and technological contexts.

Traditionally, English courts have been in favour of the postal rule in some circumstances, because the courts felt that the acceptance rule might result in each side waiting for confirmation of receipt of the last communication ad infinitum.[70] It is inevitable that the application of the acceptance rule might not promote business efficacy between parties who live far away at a time before the advancement of the postal service and the invention of paperless communications such as the telephone, telegraph and electronic means. In order to promote business efficacy at that time, it appeared to 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.[71]

In addition to reasons of business efficiency, the postal rule also gives the offeree certainty, because the offeree was at a tremendous disadvantage of not knowing whether the offer was revoked or rescinded once the offeree received the offer. If the acceptance rule applies, the offeree may also encounter the situation of not knowing the exact time of the receipt of his acceptance due to the limitation of the postal service in the nineteenth century (when the postal rule was firstly established in *Adams* v. *Lindsell* [1818] 1 B. & Ald. 681). Taking into account the normal length of time between two communications due to the limitations of communications technology and the postal service at that point in time, the courts took the view that the conduct of business would in general be better served by giving the offeree certainty.[72] The high point of the deployment of the postal rule was when it gave effect to the loss of the acceptance letter in the post. For example, in *Household Fire and Carriage Accident Insurance Co.* v. *Grant*,[73] it was held that even if an acceptance was lost and never arrived at its destination, the contract was still concluded, provided that the letter was properly stamped and the loss was not attributable to the offeree's fault. As the postal rule states that if the offeree contemplates acceptance by post the acceptance is effective once posted rather than when it is received, then 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.[74] That is, the contract is deemed to have been concluded at the

68 R. Stone (2005) *The Modern Law of Contract*, 6th edn (London: Cavendish), p. 50.
69 Ibid., p. 48.
70 *Adams* v. *Lindsell*, [1818] 1 B & Ald 681; 106 ER 250.
71 R. Stone (2005) *The Modern Law of Contract*, 6th edn (London: Cavendish), p. 49.
72 *Adams* v. *Lindsell* [1818] 1 B & Ald 681; 106 ER 250.
73 *Household Fire and Carriage Accident Insurance Co* v. *Grant* [1879] 4 Ex D 216.
74 S. Gardner (1992) 'Trashing with Trollope: a deconstruction of the postal rule in contract', *Oxford Journal of Legal Studies*, 12: 170–94.

moment the acceptance is placed into the postal system. Undoubtedly the postal rule was then created to provide certainty in contractual formation at a time when the communication system involved unavoidable delays, because the postal stamp enabled us to determine easily the time of posting an acceptance. The adoption of the postal rule has been considered to be appropriate for business if parties do not specify that the acceptance must reach the offeror in the terms, though sometimes special and temporary difficulties may render such practice unsuitable, for example when a postal service is likely to be disrupted during a time of war and a period of strike or national petrol shortage.

On the other hand, there are two major disadvantages concerning the application of the postal rule for the offeror: firstly, the offeror might assume that there was a contract and perform the contract immediately, but in fact the offer was never accepted and the letter of acceptance was never posted by the offeree; and secondly, an acceptance letter which included some amendments to the terms in the offer might never reach the offeror due to the loss of the letter, and the offeror would not be aware of those amended terms.

By contrast, the acceptance rule may resolve these disadvantages of the postal rule giving the offeror's assurance to the formation of the contract. In addition, the advancement of modern postal services in terms of recorded delivery and speed may also help resolve those concerns of the unavoidable delay in letter delivery that the postal rule has been trying to confront. Moreover, the speed of communications is further improved with the development of communications technology. Nowadays business and individuals can place an offer and accept an offer by electronic means via smart devices, such as a web application or e-mail, which takes a relatively short period of time.

In an instantaneous communication environment, there is not much time between 'the time that the offer/acceptance is sent' and 'the time that the offer/acceptance is received', which may diminish the possibility of revoking an offer and acceptance in time. Thus one of the issues which may often arise 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 received. It is obvious that there are some similarities between e-mail and the post. For instance, dispatching an e-mail is identical to dropping a letter in a red post box. Just like for the sender of a letter, the sender of an e-mail will have no control over it after having pressed the send button, as it will be transmitted to his Internet service provider (ISP). Some scholars may argue that e-mail and clickwrap agreements are different and have to be treated in a different way. It was suggested that the postal rule should apply to e-mails, while clickwrap agreements should employ the acceptance rule. In the author's view, although e-mails and clickwrap agreements are different, they have something in common that they deliver messages much faster than normal postal mailings.

3.2.6 Consideration of timing and technologies: postal mail services v. electronic mail services

In order to justify which rule (the postal rule or the acceptance rule) should apply in the online environment, there is a need to observe the technical and functional distinction between postal communications and other instantaneous forms of electronic communications, and analyse how the postal rule and the acceptance rule fit into contractual negotiations taking place by e-mail or web application.

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

- Firstly, although e-mail 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 e-mail communications.
- Secondly, current software technology makes it possible not only to determine exactly when the acceptance e-mail 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 e-mail 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 rather 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.[75] Thus, when the e-mail 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 acknowledgment of e-mail, 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.

75 R. Ong (2004) 'Consumer-based electronic commerce: a comparative analysis of the position in Malaysia and Hongkong', *International Journal of Law and Information Technology*, 12: 101–19, at p. 101.

Thus, taking into account the unique characteristics of electronic communications in comparison with traditional paper-based communications, it would be sensible to apply the acceptance rule to electronic transactions to achieve a certain degree of convenience, consistency, harmony and certainty. That is, the acceptance takes effect when it reaches the offeror. Even in the old days, English courts had already accepted that the postal rule should not be applied where it would lead to 'manifest inconvenience or absurdity'.[76] 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.[77] The acceptance rule is also employed as a common practice to validate agreements between parties in countries in the civil law system, such as China. Thus, given that the features of electronic communications and the common use of the acceptance rule in both civil and common law countries, the acceptance rule – that the acceptance becomes effective when it reaches the offeror – should be applied in electronic contracting. Although parties are free to indicate the other rule otherwise in the agreement, the acceptance rule should be deemed to be most appropriate and reasonable in particular for a click-wrap agreement, because the speed of clicking to form an agreement is often as instantaneous as oral interactions when the standard of networks and computing systems are more or less the same between two parties.

Presuming that the acceptance rule applies, the timing for the effectiveness of the acceptance as to when an acceptance reaches the offeror needs to be defined. That is, 'Is there a contract when the acceptance is received by the server or when it is actually received and read by the offeror?'[78]

3.2.7 Solution: the application of the acceptance rule

There are different views as to how the acceptance rule should apply in the context of electronic communications. For example, in Singapore, in the case of *Chwee Kin Keong* v. *Digilandmail.com Pte Ltd*, it is not disputed that it is common ground that a contract was concluded each time when an order placed by each of the appellants was followed by the recording of the transaction as a 'successful transaction' by the automated system. The system would also send a confirmation e-mail to the person who placed the order within a few minutes of recording a 'successful transaction'. In this case, the

76 *Holwell Securities Ltd* v. *Hughes* [1974] 1 WLR 155, at 161.

77 Restatement (Second) of Contracts, §64 (1979).

78 R. Ong (2004) 'Consumer-based electronic commerce: a comparative analysis of the position in Malaysia and Hongkong', *International Journal of Law and Information Technology*, 12: 101–19, at p. 101.

contract was not valid due to unilateral mistakes.[79] However, there may be two different times confirming the same message of 'successful transaction' – one is an automated response through the World Wide Web providing a note of successful transaction on the screen and the other is a confirmation letter by e-mail. It may cause confusion if one message contradicts the other. Even if two messages are the same, it may be debatable which time of the two should be considered as the timing of acceptance which validates the agreement. In practice, online traders/retailers usually advise customers that the first automated response (by the web) should be treated as 'the receipt of processing' but the second response such as a confirmation letter of delivery (by e-mail) should then be deemed to form a valid contract of sale.

Though letters of confirmation of the order and delivery by e-mail should be considered valid, the validity may be challenged if the messages are entered into the recipient's spam box instead of the inbox. In England, the case of *Bernuth Lines Ltd* v. *High Seas Shipping Ltd ('The Eastern Navigator')* affirmed the effectiveness of an e-mailed notice of an arbitration reference regardless of the fact that the recipient's staff assumed the e-mail was 'spam' and ignored it.[80] That is, an acceptance entering into a spam box should not affect the validity of service as the first party should be expecting the response from the other party within a reasonable time, therefore it should be the first party's responsibility to check the spam box.

With regard to the interpretation of 'within a reasonable time', some academics support that 'it will be prudent for the offeror to state that an e-mailed acceptance will only occur if the e-mail (1) reaches the offeror's inbox (2) during the offeror's normal working hours'.[81] The concept of 'within business hours' for the effectiveness of acceptance was based on the importance of the fact that the recipient's knowledge of the acceptance is crucial to make a valid contract.[82] In the author's view, whether or not the theory of 'within business hours' should be applicable to e-mail communications as in the case of fax and telex communications depends on whether the technology of e-mail or other high-tech communications have removed the obstacles of bringing an acceptance to the knowledge of the recipient as with ordinary fax and telex communications. Nowadays the majority of individuals should be able to receive e-mail messages at any time via an iPad, smart phone or other wireless devices.

79 *Chwee Kin Keong* v. *Digilandmail.com Pte Ltd* [2004] SGHC 71; [2005] SGCA 2.

80 *Bernuth Lines Ltd* v. *High Seas Shipping Ltd ('The Eastern Navigator')* [2005] EWHC 3020.

81 N. Andrews (2011) *Contract Law* (New York: Cambridge University Press), p. 46; M. A. Jalil (2011) 'Clarification of rules of acceptance in making business contracts', *Journal of Politics and Law*, 4 (1): 109–22, at p. 119; and see also *Schelde Delta Shipping BV* v. *Astarte Shipping Ltd (The 'Pamela')* [1995] 2 Lloyd's Rep 249 Queen's Bench: it was held an acceptance that was sent out of business hours by telex would not be effective until the opening of the office on the next business day.

82 C. Lewis (1980) 'The formation and repudiation of contracts by international telex', *Lloyd's Maritime and Commercial Law Quarterly*, 4: 433–8, at p. 43.

That is to say, with the advancement of communication technologies and devices, e-mail can be accessed anywhere at any time whereas there is a need to have a particular physical location for a fax machine or telex service to receive a message. In addition, with the rapid development of economic globalisation, e-mail communications have been used as a tool for facilitating cross-border negotiation and agreements, which often involve various parties conducting business in different time zones. Sometimes applying the 'within business hours' rule to the effectiveness of a transaction may seem to be completely out of tune with the demand of trading speed in the information society, such as in high-frequency trading, fast trade or automated transaction systems. Having said this, it does not mean that the fact of 'the recipient's knowledge of an acceptance' should be ignored. On the contrary, efforts should be made to enhance the efficiency and certainty of the receipt of an electronic communication. For example, the EC Proposed Regulation for Electronic Transactions may provide one model by removing the fear of different legal requirements in terms of formality by introducing electronic time stamping and delivery services.[83] Taking into consideration relevant factors, there are three possibilities in applying the acceptance rule in e-mail or another equivalent mode of communication:

- 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 is usually formed when the acceptance is received by the offeror's server. The server then automatically responds to it with an acknowledgment of receipt of a successful transaction. It is also possible that a contract may be formed at the later stage if the automated system only acknowledges the receipt of the request for the processing of the transaction in the first instance and the letter confirmation follows by e-mail.

It is recognisable that there is a crossing point between e-mail contracting and clickwrap agreement forming, that is the acceptance must be received and the corresponding acknowledgment must follow. It is feasible to treat e-mail and clickwrap agreement as similar modes of electronic communications in contracts. A proposal for a uniform rule on the effectiveness of an electronic acceptance may be that 'an electronic contract will be concluded when the acceptance is received and has been retrieved or read by the offeror

83 A proposal for the Regulation on 'Electronic Identification and Trusted Services for Electronic Transactions in the Internal Market', European Commission, COM (2012) 238 final.

within a reasonable time'[84] in accordance to the determination of 'the time of receipt of electronic communications'[85] in the UN Convention. 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. Appropriate technical and legal measures on electronic time stamps and electronic delivery services may be introduced to assist the determination of the effectiveness of an electronic offer and acceptance.

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 is instead open to any party X. When Party B completes the order form and agrees to the standard terms and conditions, Party A's invitation to treat becomes a firm offer. When party B clicks the button to dispatch his order form, it should be regarded as an acceptance of party A's offer, though it is likely that the contract may be formed at the later stage when the confirmation of dispatch/delivery of goods is followed by e-mail after A's checking the stock availability. The complicated issue raised here is whether party A can amend the offer after the acceptance has been received and read, or whether party B can withdraw an acceptance due to the wrong quantity ordered. These issues will be explored and examined in Chapter 4 concerning the validity of terms and conditions and Chapter 5 under error in electronic communications.

84 F. Wang (2010) *Law of Electronic Commercial Transactions: Contemporary Issues in the EU, US and China* (Oxford: Routledge), p. 48; see also F. Wang (2008) 'E-confidence: offer and acceptance in online contracting', *International Review of Law, Computers and Technology*, 22 (3): 271–8.

85 UN Convention, Article 10. 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.'

4 What are the terms and conditions?

Terms and conditions define the parties' rights and liabilities in contracts. It is important that the underlying commercial contract terms and conditions clearly reflect the negotiated terms and conditions agreed by both parties. A poorly drafted contract increases the risk of misunderstanding and commercial disputes which may give rise to payment or performance delays, compensation and warranty disputes, etc.

The number of terms and conditions is decided in accordance with the importance of the transaction. For example, large-scale transactions often produce contracts of considerable length and complexity including standard form clauses, such as exclusion and limitation clauses. Many companies spend substantial sums of money on legal advice in relation to the drafting of their standard terms of business. It is always prudent to read the available terms and conditions and take adequate steps to ensure that those terms and conditions are incorporated into the contracts which they conclude.

Key legal issues in the context of terms and conditions include, for example, the duty to make the text available, the awareness of the types of terms (i.e. express terms and implied terms), the nature of terms (i.e. conditions, warranties and innominate terms), the selection of contractual language and the battle of the forms.

It is debatable whether there are uniform rules concerning the methods and requirements of 'making contractual terms and conditions available' and 'incorporating terms and conditions into the contract' in international legal instruments such as the CISG and UNIDROIT Principles.[1] Although it is suggested that 'using the CISG and the Principles together makes it possible to create a complex regulation of contractual relationships in the international

1 See the United Nations Convention on Contracts for the International Sale of Goods 1980 (CISG) and the UNIDROIT Principles of International Commercial Contracts 2010 (UNIDROIT Principles).

sale of goods',[2] both instruments do not provide a specific provision regarding 'the availability of contractual terms and conditions'. It is arguable that the CISG (Article 8) provides a relevant provision regulating the manner of negotiating and incorporating terms and condition[3] that 'statements made by and other conduct of a party are to be interpreted according to his intent where the other party knew or could not have been unaware what that intent was'. It is noted that some other relevant provisions can also be found in the CISG and UNIDROIT Principles applying to 'the incorporation of terms and conditions', though they are geared towards the incorporation of standard terms and the battle of the forms. Moreover, the CISG provides a gap-filling procedure in Article 7 so that it is possible that the substantive issues regarding the availability and incorporation of terms and conditions are governed by national laws instead. For example, the question of the incorporation of standard contract terms had to be answered in accordance with general Dutch Civil Code provisions on offer and acceptance because the provision of standard terms in the Dutch Civil Code is only applicable to domestic contracts.[4]

In the information society, it seems to be even more crucial to adopt consistent and fair international standards of 'making terms and conditions available online' and 'incorporating them into the electronic agreement', taking into account the features of electronic communications and the nature of cross-border transactions. Thus, according to Article 7 of the CISG, other international legislation such as the UN Convention on the Use of Electronic Communications in International Contracts 2005 (hereafter 'the UN Convention) and regional or national instruments can in theory play a role in filling a gap among traditional international instruments such as the CISG, though the UN Convention also lacks provisions concerning the availability and incorporation of contractual terms and conditions.

4.1 Availability of terms and conditions

The availability of terms and conditions (T&C) is of great importance prior to and after the conclusion of a contract. This is to ensure the fairness between two parties, in particular in the context of the usage of standard terms. Once terms and conditions are agreed by the parties, they become effective and binding

2 J. Kotrusz (2009) 'Gap-filling of the CISG by the UNIDROIT Principles of International Commercial Contracts', *Uniform Law Review*, 26 (1–2): 119–63, at p. 145; and *see* also the 45th Session UNCITRAL (New York, 25 June – 6 July 2012) endorsed the 2010 edition of the UNIDROIT Principles.

3 F. Lautenschlager (2007) 'Current problems regarding the interpretation of statements and party conduct under the CISG – the reasonable third person, language problems and standard terms and conditions', *Vindobona Journal of International Commercial Law and Arbitration*, 11 (2): 259–90.

4 A. Janssen (2005) 'The Dutch Supreme Court and the incorporation of standard contract terms in international sales contracts', *Uniform Law Review*, pp. 901–5, at p. 905. See also *Vergo Kwekerijen* v. *unknown*, Hoge Raad der Nederlanden, Netherlands, 28 January 2005, Supreme Court.

unless the parties can prove that there were vitiating factors such as mistakes or misrepresentation.

The deployment of appropriate methods of making T&C available is required in order to justify an opportunity provided clearly for the contracting parties to read the terms and conditions so that the consent which the parties may give to the offer can constitute an informed consent of incorporating those T&C into the agreement. In the old days, terms were usually made available in writing or first discussed in a meeting before being reduced into writing. In electronic contracting, the T&C are usually displayed on a website, via a hyperlink address, through an adjacent scroll box, in a downloadable PDF file or word document, or in an e-mail message.

Sometimes it is likely that after clicking the 'I agree' or 'submit' button or ticking a checkbox, the 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, where standard T&C are inalterable, parties asked to 'agree' to the terms in some instances will have no easy alternative other than to submit.[5]

Occasionally it is also likely that there may be a conflict between written agreements and online agreements regarding the same transaction. For example, in the US, in the case of *Fadal Machining Centers, LLC* v. *Compumachine, Inc.*, the terms and conditions on Fadal's website provided that within six months after any act or omission in controversy, claims or disputes 'arising out of or related to this agreement, or the breach thereof' shall exclusively be submitted to arbitration in Los Angeles, California under the Commercial Arbitration Rules of the American Arbitration Association (AAA).[6] However, the distributorship agreement in writing designated the US District Court for the Central District of California as the forum to resolve disputes. The Ninth Circuit (US Court of Appeals) upheld a district court's enforcement of an arbitration clause included in a manufacturer's online terms and conditions regardless of a conflicting distributorship agreement as the written agreement provided that Fadal would unilaterally establish 'the terms of sale … from time to time'.[7]

From time to time, high-tech or e-commerce companies will also revise or amend the T&C for the use of online services in order to be in line with updated or new services resulting from technology innovation. Users should be informed about those changes and provided with the revised terms and conditions. The questions are in what manner the revised T&C should be displayed, what would constitute an informed notice to users and how is

5 J. R. Maxeiner (2003) 'Standard terms contracting in the global electronic age: European alternatives', *Yale Journal of International Law*, 28 (1): 109–82, at p. 114.

6 Memorandum for *Fadal Machining Centers, LLC* v. *Compumachine, Inc.*, No. 10-55719 (9th Cir., Dec. 15, 2011).

7 Ibid., p. 3.

informed consent to be collected from users to the revised terms and conditions. Although it is expected that some users do not read terms and conditions properly before they give their consent, it is the manufacturers' or sellers' responsibility to provide information on changes in an appropriate and effective manner. For example, in China, in the case of *Ying Mao Company* v. *Tian Yuan Company (Metarnet Technologies Co., Ltd)*,[8] Ying Mao Company registered a free 50 GB storage e-mail account with the Tian Yuan Company but in 2001 Tian Yuan informed all users of a reduction in the free storage from 50GB to 5GB temporarily. Ying Mao claimed that Tian Yuan breached the agreement for the e-mail service and requested Tian Yuan to restore the original capacity of the e-mail account. Both the People's Court for Haidian District Beijing and the Court of Appeal in the Beijing No. 1 Intermediate Court held that Tian Yuan did not breach the service contract by adjusting the capacity of the e-mail account as Tian Yuan had announced this decision on its website to all users which fulfilled the obligation of informing users ('duty to call attention') about the changes of service terms according to the e-mail service agreement. Thus Tian Yuan's amendment to the e-mail service agreement did not infringe the provisions concerning standard terms in the China Contract Law (Articles 39, 40, 41, 52 and 53).

Furthermore, if the amendment of terms and conditions is displayed on a website via a hyperlink without the possibility of printing or downloading, should this be deemed to be a valid form to fulfil the duty to inform? There is a growing concern over the validity of terms and conditions which are displayed via a hyperlink on a website. It is noteworthy that the primary nature of a hyperlink is a clickable link to the destination address, while the primary function of a hyperlink is to help users to go to the information page. A hyperlink acts as an indexed tool which is identical to indexes in the library or bookstore. According to the primary nature and function of a hyperlink, the provision of hyperlinking (either surface linking or deep linking) should be deemed to be the provision of a tool that provides the location address and access to information in principle. From a legitimacy perspective, a hyperlink address may be used as: (1) another form of citation or quotation for published and copyrighted work in particular in scientific work for educational purposes; or (b) another format of providing additional information/reference for business. Correspondingly, hyperlinking itself may not immediately infringe others' rights or generate invalid agreements. In other words, the action of hyperlinking should not be treated as a sole/direct indicator, measurement or benchmark for determining illegal activities and unlawful procedure. For example, in the EU, in the recent ECJ case regarding distance selling – *Content Services Ltd* v. *Bundesarbeitskammer*, it appeared that

8 '*Ying Mao Company* v. *Tian Yuan Company (Metarnet Technologies Co., Ltd)*, Case of Guaranty Contract Resource Right Dispute', *Gazette of the Supreme People's Court of the People's Republic of China*, 6, 2006, p. 207.

a hyperlink itself did not determine the validity of the terms and conditions,[9] though it was concerned whether the terms and conditions made available via a hyperlink would affect the effectiveness of the availability and incorporation of those terms and conditions.

It is, therefore, important to implement a harmonised standard of 'the availability of terms and conditions' in electronic communications. In response to the matters concerned, some regional or domestic laws provide relevant provisions as to the manner of making T&C available. It is a common requirement 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, though some may not cover the issue regarding the consequences of the failure to comply with requirements of availability of T&C electronically. In the EU, US and China, references can be found as follows.

In the EU, the EC Directive on Electronic Commerce (Article 10(1)(b)) requires that the concluded contract should be filed by the service providers, and it must be *accessible*. Furthermore, it stipulates 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' (Article 10(3)). However, the EC Directive on Electronic Commerce does not provide the solution for determining the consequences of a failure to provide the stipulated information. In addition to the requirement of accessibility, storage and reproducibility, the EC Distance Selling Directive (replaced by the EC Directive on Consumer Rights in 2014) also provides relevant provisions in order to enhance consumer protection. The EC Distance Selling Directive (Article 4(20)) (replaced by Article 6(1) of the EC Directive on Consumer Rights in 2014) specifies that information in relation to the sale of goods or provision of services shall be provided to consumers 'in a *clear and comprehensible* manner in any way *appropriate* to the means of distance communication used' to enable them to give informed consent. Moreover, the EC Distance Selling Directive (Article 5(1)) (replaced by Article 8(1) of the EC Directive on Consumer Rights in 2014) requires that 'the consumer must receive written confirmation or confirmation in another *durable medium available and accessible* to him of the information' prior to the conclusion of the contract, during the performance of the contract and at the latest at the time of delivery. The recent Proposed European Common Sales Law (Article 24(4)) also proposes that 'the trader must ensure that the contract terms … are made available in alphabetical or other intelligible characters and on a durable medium by means of any support which permits reading, recording of the information contained in the text and its reproduction in tangible form.'[10] The form of a durable medium was interpreted

9 ECJ Case C 49/11, *Content Services Ltd* v. *Bundesarbeitskammer*, 5 July 2012.
10 Proposed European Common Sales Law 2011, Article 24(4).

in the case of *Content Services Ltd* v. *Bundesarbeitskammer*.[11] It was concluded that a webpage on a website should not be considered as a valid form of a durable medium.

In the US, UETA (Sections 8(a) and 8(c)) indicates that 'an electronic record is not capable of retention by the recipient if the sender or its information processing system inhibits the ability of the recipient to *print or store* the electronic record', which may result in an electronic record being 'not enforceable against the recipient'. It also specifies that the otherwise applicable substantive law will not be overridden by this Act and it is subject to other law that requires a record to be posted or displayed in a certain manner (Section 8(b)). This is to ensure consistency with other law, the fairness of an agreement and the availability of information for later reference. It was explained under the comment note of the UETA (Section 8) that 'the policies underlying laws requiring the provision of information in writing warrant the imposition of an additional burden on the sender to make the information available in a manner which will *permit subsequent reference*'.[12]

In China, the China Electronic Signatures Law (Articles 4, 5(1) and 6(1)) also considers the purpose of '*for reference*' as indicated in the UETA that 'a data message, which can give *visible and effective expression* to the contents carried and can readily be picked up *for reference*, shall be deemed to be the written form which conforms to the requirements of laws and regulations'.

At the international level, the UNCITRAL Model Law on Electronic Commerce (Article 6) also recognises the significance of information available 'for subsequent reference', providing that 'where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable *for subsequent reference*'. The UN Convention on the Use of Electronic Communications in International Contracts (hereafter 'the UN Convention') also emphasises such importance providing 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*' (Article 9(2)). The weight of this element can be further evidenced by another two provisions – Articles 4 and 13 of the UN Convention, in particular that Article 13 proposes a specific title of the 'Availability of Contract Terms'. The UN Convention (Article 4(b)) stipulates that 'where the law requires that a communication or a contract should be made available or retained in its original form, that information is *capable of being displayed* to the person to whom it is to be made *available*.' The specific provision of 'Availability of Contract Terms' (Article 13) particularly clarifies that 'nothing in this

11 ECJ Case C 49/11, *Content Services Ltd* v. *Bundesarbeitskammer*, 5 July 2012.

12 UETA, Section 8 – Comment para. 3. Available at: http://www.uniformlaws.org/shared/docs/electronic%20transactions/ueta_final_99.pdf (last accessed 30 June 2013).

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.' However, the UN Convention does not intend to use the specific provision of 'Availability of Contract Terms' to harmonise the international standard of best practices; instead it serves as 'a reminder for parties that the facilitative rules on the Convention did not relieve them from any obligation they may have to comply with domestic legal requirements that may impose a duty to make contract terms available'.[13] That is, the UN Convention does not impose any requirement for contracting parties to make available the contractual terms in any particular manner as well as any consequence for failure to perform the duty.

The UN Convention preserves the application of domestic law, which means that the substantive issues of the availability of contract terms will still be subject to relevant national laws, in particular consumer protection regulations.[14] Although it recognises that creating 'specific obligations seems to be an interest in enhancing legal certainty, transparency and predictability in international transactions concluded by electronic means',[15] it is asserted that introducing a duty to make contract terms available would 'result in imposing rules that did not exist in the context of paper-based transactions'.[16] Subsequently no formulation is provided for an appropriate set of possible consequences for failure to comply with a requirement to make contract terms available in the UN Convention.[17] It is notable that, subject to domestic laws, there may be a wide variety of consequences for failure to make the T&C available such as an administrative offence, a fine, a condition on the effectiveness of contract or a court order of enforcement.[18]

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 that the issue of making the T&C available should be compulsory.

With regard to the particular manner in which the terms should be deemed as being validly made available, a harmonised standard of technical measures is also of the essence to ensure the fairness for the conclusion and performance of a contract. It is sensible for the UN Convention to introduce technology-neutral technical means for storage or printing of the contract terms in a way

13 Explanatory Note 2007, p. 72, para. 222.
14 See A/CN.9/509, para. 63.
15 Explanatory Note 2007, p. 71, para. 217.
16 Explanatory Note 2007, p. 72, para. 221; see also A/CN.9/509, para. 123.
17 See A/CN.9/571, para. 179
18 Explanatory Note 2007, p. 71.

that allows for safe storage and reproduction. For example, such means may be by a display on the website with a function for printing, by uploading a PDF file or Word document for downloading from the network, by a digital copy in the users' online account for later access, by a confirmation e-mail or by a form for requesting hard copies from merchants.

As to valid consent, it is common that national laws require businesses or merchants to obtain users' consent to the T&C before they become effective. It is also normal in most countries that the modification of the T&C should also be notified and accepted by the counter-parties in order to become part of the contract. With regard to the issue of when knowledge of the T&C shall be gained or consent should be given, there are two major views: the majority of countries require prior knowledge before the conclusion of a contract by explicitly expressing consent, or knowledge at least, at the time of contract conclusion[19] on the receipt of the contract or agreement by giving implied consent, while the other view is that an e-market participant shall in principle be bound by the T&C if, at the time of agreement, he was aware or should have been aware of such terms using ordinary care.[20] It is noteworthy that meeting the requirements of the availability of contract terms is the prerequisite to fulfil the requirements of the awareness of the contract or sale agreement. In electronic contracting, if it can be ensured that contract terms can be made available and accessible at any time, it could be much more efficient and convenient than offline contracting. For example, when a wholesaler goes to Makro Whole Sale Store to order products and pays for them at the till, it is doubtful that they will actually check the small print of the T&C on the back of the receipt. Alternatively, if a wholesaler purchases products through Makro's website where a tool for viewing and selecting clauses of the T&C is provided, it is more likely that the wholesaler will read and select the T&C before the conclusion of the contract.

Last but not least, it is also prudent to implement fair, reasonable and appropriate legal measures and sanctions for non-compliance in the UN Convention. It is necessary to have a harmonised standard in terms of legal measures, though there is no need to have a provision proposing a specific figure for a fine or other specific penalties, as this should be subject to substantive laws in different countries.

4.2 Incorporation of terms and conditions

How terms and conditions are validly and effectively incorporated into a contract is usually subject to domestic contract law. Traditionally, most countries recognise three main methods of incorporation of contract terms: by

19 'Legal Study on Unfair Commercial Practices within B2B e-markets – Final Report', European Commission Study ENTR/04/69 (May 2006), p. 73–4.

20 *Sweeny* v. *Mulcahy* [1993] ILRM 289.

signature, by notice/reference and by course of dealing (or by custom). In an increasingly electronic transaction environment, terms and conditions of sale or purchase may be expected to be incorporated electronically either via automated transaction systems, e-mail communications or other electronic means. The incorporation of terms and conditions by electronic means challenges the validity of traditional methods of incorporation. Thus interpretation of the existing rules is required in order to adapt them to determining the effectiveness of terms and conditions incorporated by electronic means.

4.2.1 Incorporation by signature

The easiest (and most certain) method of incorporating terms and conditions is through signature. For example, in the leading English case of *L'Estrange* v. *F. Graucob Ltd*,[21] a cafe owner bought a cigarette vending machine and signed a sales agreement which she did not read. A term of this agreement, which was 'in regrettably small but quite legible' form, said that the machine did not need to work and that all statutory implied terms were not to apply. The machine did not work. The cafe owner sued to get her money back, claiming that Section 14(2) of the Sale of Goods Act had been breached. The court held that the cafe owner failed, even though Section 14(2) of the Sale of Goods Act had clearly been breached. The claimant had signed the agreement and so she was bound by it. In the information society, electronic signatures have been deemed to have the equivalent effect of 'written signatures'. Inserting a name in an encrypted e-mail message or clicking an 'I agree' button on a website may constitute a valid form of signature and thus validly incorporate terms into a contract. For example, in the American case of *Moore* v. *Microsoft Corporation*, it held that clicking an 'I agree' button was sufficient for the terms and conditions to be incorporated.[22]

4.2.2 Incorporation by notice/reference

The second main method of incorporating terms and conditions into a contract is incorporation by notice or by reference. Parties can be bound in circumstances where they were given reasonable notice of terms. For incorporation by notice to be valid, essentially three factors have to be satisfied: (1) within good time; (2) in a contractual document; (3) reasonable steps have to be taken to bring the contractual terms to the notice of the other party. In a leading English case of *Olley* v. *Marlborough Court Limited*, the terms and conditions excluding liability for loss or damage to property which appeared on the back of a hotel door were held not to be incorporated. As the contract for a room had been agreed at the hotel front desk, the terms – which were not

21 *L'Estrange* v. *F Graucob Ltd* [1934] 2 KB 394.
22 *Moore* v. *Microsoft Corporation* (15 April 2002) NY Sup. Ct. App. Div. 2nd Dept.

highlighted until the customer reached their bedroom – could not be said to have been incorporated.[23] That is, the awareness of the terms is essential to the effectiveness of the incorporation of contract terms. Similarly in another traditional English case of *Chapelton* v. *Barry Urban District Council*, the Court of Appeal held that the terms and conditions for the hire of deckchairs (that were printed on the back of the ticket) and which the owners of the deckchairs attempted to rely upon were not enforceable as the ticket was simply a receipt for the money paid for the hire of the chair.[24] It is obvious that the offeree's actual awareness of contract terms is the prerequisite before those terms can be validly and effectively incorporated into the contract.

In an online environment, how to ensure that the offeree is aware of electronic contract terms before terms are concluded is the focal point of the effectiveness of the incorporation of electronic contract terms by notice or reference. It is suggested that there are generally two approaches in response to the incorporation of standard terms: one is that 'the terms enter the contract automatically unless the other party promptly objects to their inclusion' and the other is that 'something more than failure to object is necessary for the inclusion of the standard terms'.[25] That is, the party must be aware of the standard terms before they can be incorporated into the contract.

An online PDF file containing terms and conditions which are displayed on a website may amount to an actual awareness of information for users but a brief statement on a website may not be sufficient to be treated as a term. For example, in the English case of *Gary Patchett* v. *Swimming Pool and Allied Trades Association Limited (SPATA)*, Mr and Mrs Patchett obtained details of installers from a dropdown list on SPATA's (a company's) website and contracted with one of them, Crown Pools Limited, to build a swimming pool in their garden. The SPATA website stated that members were fully vetted (with checks on their financial record and experience and an inspection of their work) and that they benefited from a bond and warranty scheme known as SPATASHIELD. SPATA's website also included a reference to and encouraged people to obtain a copy of an information pack. It turned out that Crown was not a full member and therefore had not been vetted and did not benefit from the SPATASHEILD scheme, but Mr and Mrs Patchett claimed that they relied on the statements on the website as they did not check the information pack. The Court of Appeal held that it was reasonable that a customer would be expected to look at the website as a whole and obtain the relevant information pack, therefore SPATA was not liable for the error on the website as all information was correctly recorded in an information pack confirming the terms of cover.[26] In other words, SPATA had performed its

23 *Olley* v. *Marlborough Court Limited* [1949] 1 KB 532.

24 *Chapelton* v. *Barry Urban District Council* [1940] 1 KB 532.

25 L. A. DiMatteo (2011) 'Critical issues in the formation of contracts under the CISG', *Belgrade Law Review*, 59 (3): 67–83, at p. 78.

26 *Gary Patchett* v. *Swimming Pool and Allied Trades Association Limited (SPATA)* [2009] EWCA Civ. 717.

duty to inform as 'the website should not be taken as inviting reliance without further enquiry, that is without applying for and reading the information pack referred to in paragraph 8 of the website',[27] whereas 'the appellants had been grossly negligent in failing to make enquiries as to the availability of SPATASHIELD insurance.'[28] This is identical to a situation when customers purchase travel insurance on a website. It is sensible that customers are expected to download the PDF files of 'the fact sheet' and 'terms and conditions' and read them before they complete the purchase of insurance.

Terms may also be incorporated into a contract by reference via e-mail communications and their attachments. In the US, in the case of *Golden Valley Grape Juice and Wine, LLC* v. *Centrisys Corporation et al.*, the offer was made by e-mail providing the sale quotes, which was an adequate office pursuant to the CISG. In the same e-mail there were three attachments: 'the General Conditions', 'the Warranty' and 'the Banking Information'. The court ruled that the General Conditions were not attached to just any correspondence but were provided *contemporaneously* with the sales quotes and thus were part of the contract. Although a forum selection clause was included in the General Conditions and should in theory be considered part of the contract, the wording was too broadly expressed and thus invoked.[29]

It is also advisable that a notice/reference on a website must be *reasonable* and *adequate* for the terms to be effectively incorporated. For instance, in the US, in the case of *Manasher* v. *NECC Telecom*, the court held that an arbitration clause found in the defendant's online terms and conditions was not incorporated into the contract terms by reference, because an arbitration clause added in an amended terms and conditions was unconscionable – the online terms were placed and referenced in the fifth statement of the second page of the defendant's invoice and in ambiguous language.[30] In contrast, in the case of *Paola Briceño* v. *Sprint Spectrum, L.P.*, it was confirmed that:

> Sprint printed a 'Notice of Changes' on the front of the June 16, 2003 invoice that it mailed to Briceño. This notice informed her that amendments to the original Terms and Conditions were posted on Sprint's website. Briceño stated that she never read any of the original or amended Terms and Conditions, either on the internet or in hard-copy, because it was 'not important' to her. She also stated that she saw the 'Terms and Conditions of Service' internet link, but did not care to click it.[31]

27 [2009] EWCA Civ. 717, para. 51.

28 [2009] EWCA Civ. 717, para. 58.

29 *Golden Valley Grape Juice and Wine, LLC* v. *Centrisys Corporation et al.*, Case No. CV F 09-1424 LJO GSA, 21 January 2010 (the United States District Court of the Eastern District of California).

30 *Manasher* v. *NECC Telecom*, No. 06-10749, 2007 WL 2713845 (E.D. Mich. 2007).

31 *Paola Briceño* v. *Sprint Spectrum L.P.*, 911 So.2d 176, 177–80 (Fla. Ct. App. 2005), in the District Court of Appeal of Florida, Third District.

The court held that a customer would be bound by the amended terms and conditions if the customer was properly informed of them though did not read them. In particular there was no evidence that Sprint concealed or attempted to conceal the aforementioned original or amended terms and conditions.[32] Thus proper notice of modified terms is so important that it is required for consent to be effective.[33]

In order to further protect consumers' rights online, the consumer must receive written confirmation or confirmation in another available durable medium. In the EU, the judge in the recent ECJ case of *Content Services Ltd* v. *Bundesarbeitskammer* provided an interpretation on whether information (such as terms and conditions) that is available via a hyperlink on a website should be effective and enforceable. On 5 July 2012 the Court ruled that:

> Article 5(1) of Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts must be interpreted as meaning that a business practice consisting of making the information referred to in that provision accessible to the consumer *only via a hyperlink on a website* of the undertaking concerned does not meet the requirements of that provision, since that information is neither 'given' by that undertaking nor 'received' by the consumer, within the meaning of that provision, and *a website* such as that at issue in the main proceedings *cannot be regarded as a 'durable medium'* within the meaning of Article 5(1).[34]

It was evidenced that a hyperlink itself did not determine the validity of the terms and conditions, but the problem was that a website itself referred to by a hyperlink could not be deemed to be a 'durable medium'. This is because information on a website (i.e. the content of a webpage) can be altered constantly. If a hyperlink leads to a PDF document which can be stored, accessed and reproduced, such PDF document/file can be transferred to a 'durable medium' and thus should meet the requirements.[35] Or if the technology is developed for a website to ensure that information, can be stored, accessed and reproduced on that website by the consumer during an adequate period, this can then meet the requirements of 'a durable medium'.[36]

32 11 So.2d 176, 177–80 (Fla. Ct. App. 2005), p. 8.

33 B. Casady (2009) 'Electronic pitfalls: the online modification of ongoing consumer service agreements', *Shidler Journal of Law, Commerce and Technology*, 5: 12.

34 ECJ Case C 49/11, *Content Services Ltd* v. *Bundesarbeitskammer*, 5 July 2012.

35 F. Wang (2013) 'Hyperlinking: debate on contract, IP and database regulation', *Intellectual Property Forum* (a quarterly journal published by the Intellectual Property Society of Australia and New Zealand), 93: 85–9.

36 ECJ Case C 49/11, para. 48.

4.2.3 Incorporation by course of dealing/by custom

The third common method for the incorporation of contract terms is by course of dealing or by custom. The incorporation of contract terms by course of dealing is only possible when a course of dealing is regular and consistent.[37] For example, if standard terms are regularly and consistently used between two commercial customers, it will be unreasonable to deny the awareness of those sets of standard terms. In the recent English case *Allen Fabrications Limited* v. *ASD Limited*, none of the contractual documents made reference to either party's standard terms and conditions.[38] As there had been over 250 transactions between the parties which in each case involved the sending to the plaintiff of an advice note and an invoice,[39] and both parties had their own sets of standard terms, it evidenced that 'the whole thrust of his patently honest evidence was that he well understood the existence of such terms and why they were there, why they were needed and why a buyer would take the risk of being bound by them.'[40] On that footing the seller only needed to satisfy the normal 'notice' test for incorporation and course of dealing, which they did.[41] Thus there was a course of dealing sufficient in the ordinary way to entail the incorporation of the seller's standard terms because of the numerous invoices.[42]

With regard to the incorporation of electronic contract terms by course of dealing, in *University of Plymouth* v. *European Language Centre Limited* [2009], the European Language Centre used accommodation at the University of Plymouth for their summer language classes. The number of beds available was reduced to 100 at the end, though it was estimated that about 200 beds would be available through e-mails and over the telephone during the period of enquiry. The language centre sued the university, arguing that a contract was in existence for 200 beds, per the earlier e-mail and telephone communication. The Court of Appeal held that a contract had not been entered into and they had merely been negotiating prior to formalising the arrangement into a contract after it looked at the record of the entire communication between the parties. The incorporation by a course of dealing was not applicable as in previous years the final arrangement would be concluded in a detailed contract.[43] Thus it is understandable that a course of dealing must be regular and consistent and 'onerous or unusual terms should be brought specifically to the buyer's attention',[44] otherwise they will not form part of any course of dealing.

37 *McCutcheon* v. *David MacBrayne Ltd* [1964] 1 WLR 125.
38 *Allen Fabrications Limited* v. *ASD Limited* [2012] EWHC 2213 (TCC), para. 17.
39 [2012] EWHC 2213 (TCC), para. 13.
40 [2012] EWHC 2213 (TCC), para. 30.
41 [2012] EWHC 2213 (TCC), para. 64.
42 [2012] EWHC 2213 (TCC), paras 13 and 66.
43 *University of Plymouth* v. *European Language Centre Limited* [2009] EWCA Civ. 794.
44 [2012] EWHC 2213 (TCC), para. 54.

5 What are the vitiating factors?

5.1 Error in electronic communications

Error in electronic communications is often connected with the concepts of mistake and misrepresentation in traditional contract law. On an electronic commerce platform, pricing errors may occur accidentally due to the automated and speedy features of the Internet. Misleading statements in terms of product description can also easily occur in online shopping as products cannot actually be seen, touched or tested by buyers. 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.[1] In Singapore, in the case of *Chwee Kin Keong and Others* v. *Digilandmail.com Pte Ltd*, Digiland advertised for sale a Hewlett-Packard laser printer with the description 'HPC 9660A Color LaserJet 4600' priced at $3,854 (goods and services tax (GST) not included) on its website (the D website) and the HP website. It was priced at $3,448 on the DIL website.[2] The price for the printer was accidentally altered to just $66 on all three websites due to an error which occurred in DIL and the product description was also inadvertently altered to just the numeral '55'.[3]

When an online error happens, traditional concepts of mistake and misrepresentation are interpreted to determine the situation.[4] One of the legal challenges in resolving online errors is that online buyers are in a difficult position to prove any technical mistakes or misleading statements on an e-commerce website, because online buyers have limited technical controls over their online transactions, and the website controller (in particular when the seller controls the website) can update or amend the misleading statement on

1 'Time to get real about the net', BBC News, 21 March 2003. Available at: http://news.bbc.co.uk/1/hi/technology/2872429.stm (last accessed 30 June 2013).

2 *Chwee Kin Keong and Others* v. *Digilandmail.com Pte Ltd* [2005] SGCA 2, para. 4.

3 [2005] SGCA 2, para. 5.

4 For example, in the case of *Chwee Kin Keong and Others* v. *Digilandmail.com Pte Ltd* [2005] SGCA 2, the doctrine of unilateral mistakes is employed to determine the effect of online price error.

the web page at any time. Some factors have been recognised in judicial cases in recent years in relation to the effectiveness of the incorporation of contract terms, for instance a website cannot be deemed to be a durable medium to record contractual terms.[5]

In the traditional common law system, mistake is when parties make errors in the subject matter or terms of the contract as to the title, quality or quantity, etc. On the other hand, misrepresentation refers to a false statement of fact that induces the other party to enter into a contract. In traditional contract laws, mistake can make a contract void while misrepresentation can make a contract voidable. In a civil law system as in China, the contract will be subject to amendment or cancellation if the contract was concluded due to a material mistake.[6]

It is noticeable that a mistake may occur at the time of making the contract. The first stage in approaching an issue is to identify the type of mistake in question. It is commonly known that there are three types of mistake: common mistake, mutual mistake and unilateral mistake.[7] Mistakes should be fundamental so as to constitute a void contract.[8] Broadly, there are five situations that will give rise to a common mistake:

- mistake as to the existence of the subject matter;
- mistake as to the identity of ownership;
- mistake as to the possibility of performance;
- mistake as to the quality of the subject matter; and
- mistake as to the quantity of the subject matter.

The first three types of common mistake are most likely to make a contract void, but common mistake as to the quality of the subject matter will usually not make the contract void. As Lord Atkin said, mistake as to quality 'will not affect assent unless it is the mistake of both parties, and is as to the existence of some quality which makes the thing without the quality essentially different from the thing as it was believed to be.'[9] Common mistake as to the quantity is likely to make a contract void. For example, in the case of *Cox* v. *Prentice*, a silver bar was sold under a mistake as to its weight. The buyer obtained a verdict for damages for the difference in value between the weight of the bar as it was and as it was believed to be. The court added that the buyer could have recovered back the price he paid for the bar, which may suggest that he

5 ECJ Case C 49/11, *Content Services Ltd* v. *Bundesarbeitskammer*, 5 July 2012.
6 China Contract Law 1999, Article 54.
7 Common mistake is also known as bilateral mistake and occurs when both parties make the same mistake. Mutual mistake occurs when the two parties mean different things. Unilateral mistake occurs when one of the parties is mistaken about some fundamental fact and the other party knows or should know this.
8 *The Great Peace Shipping Ltd* v. *Tsavliris Salvage (International) Ltd* [2002] 3 WLR 1617.
9 *Bell* v. *Lever Brothers Ltd* [1932] AC 161; see also *Leaf* v. *International Galleries* [1950] 2 KB 86.

had the option of treating the contract as void for mistake.[10] As to the effect of unilateral mistake, it is possible that a unilateral mistake as to either the person or the terms of the contract can render an agreement void but such mistake should be 'fundamental' to have that effect.

In contrast, misrepresentation is a misleading pre-contractual statement or an unambiguous false statement of fact. To constitute a misrepresentation, the statement must have been addressed to the party misled and induced that other party to enter into a contract. It should also be about a false statement to a material fact. A claim for misrepresentation will render the contract voidable (not void) and the consequences can be damages and/or rescission, depending on state of the mind of the misrepresentor.

Commonly there is a four-step approach to the determination of a misrepresentation:

Step 1. Distinguish a term of a contract from a representation.
Step 2. Identify an actionable misrepresentation.
Step 3. Differentiate between the different types of misrepresentation.
Step 4. Analyse the remedies for misrepresentation.

There are also three types of actionable misrepresentation:

- fraudulent misrepresentation;
- negligent misrepresentation; and
- innocent misrepresentation.

In the information society, error in electronic communications usually refers to input mistakes or the input of a false statement (misrepresentation) by electronic means. The determination of mistake and misrepresentation occurring in electronic communications should in theory be similar to that at the time of forming a traditional contract. In practice, appropriate technical measures should be made available to amend an electronic error, and the specific interpretation of traditional concepts may need to be adapted to the new characteristics of an online error. For example, in the case of *Seatbooker Sales Limited* v. *Southend United Football Club*, the original contract for an Internet ticket sales service was valid as no mistake and misrepresentation was found.[11] It is obvious that error in electronic communications should include both electronic input mistakes and electronic false statement. The traditional concepts of mistakes and misrepresentation are used to apply to electronic errors.

One of the features distinguishing online methods of communications from traditional media is that software now assumes an instrumental role in

10 *Cox* v. *Prentice* [1815] 3 M & S.
11 *Seatbooker Sales Limited* v. *Southend United Football Club* [2008] EWHC 157.

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.[12] Thus there are differences between electronic contracts and paper-based contracts in the process of forming a contract. To determine the effect of 'error in electronic communications' compared with 'the traditional mistake and misrepresentation in contracts', it is necessary to consider whether there is something more that we need to protect beyond the existing contract law, when errors occur in electronic commercial transactions.

5.1.1 Current legislation concerning electronic error

International approach

Article 14 of the UN Convention on the Use of Electronic Communications in International Contracts (hereafter 'the UN Convention') provides 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 two main conditions on withdrawing the portion of electronic communications in which an input error was made.

12 J. Savirimuthu (2005) 'Online contract formation: taking technological infrastructure seriously', *University of Ottawa Law and Technology Journal*, 2: 105–43, at p. 126.

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.[13] 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 of value from the goods or services.'[14]

EU approach

Compared to 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.[15] 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:[16]

- 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.'

In contrast, the EC Distance Selling Directive (replaced by the EC Directive on Consumer Rights in 2014) does not have a specific provision to regulate

13 Explanatory Note 2007, p. 74.
14 The UN Convention 2005, Article 14.
15 EC Directive on Electronic Commerce, Article 10.
16 Ibid.

'error in electronic communications' but a provision granting 'rights of withdrawal' to consumers. The provision of 'rights of withdrawal' gives consumers rights to return goods without any penalty and without giving any reason,[17] which can be used in a situation where there is an error in electronic orders.

US approach

Section 153 of the Second Restatement of Contracts 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 Section 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.

Section 10 of the Uniform Electronic Transactions Act (UETA) 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.

17 EC Distance Selling Directive, Article 6(1); and see also the EC Directive on Consumer Rights 2011, Articles 6 to 16.

(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, Section 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 Section 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 '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 for 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 China Contract Law, 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.[18] That is, the terms 'misconduct', 'fairness', 'fraud' and 'exploitation' have been introduced to determine the validity of a contract and the legality of modification or revocation of the contract in China Contract Law. Such terms are equivalent to mistake and misrepresentation in common law.

5.1.2 Obstacles in regulating electronic error

There are four major concerns regarding electronic mistakes and misrepresentation in expression:

- First, who should be responsible for the mistake or 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 the withdrawal or avoidance of electronic communications affected by errors?

Two of the main features of electronic communication are that they are instant and automatic. 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 actions in reliance of the mistake.[19] For example, suppose A has offered B (business partner) $20 per product 'Z' by e-mail, but immediately A realises that the price has increased in line with inflation, thus A sends another email to inform B that the price has to change to $28 per product Z. Will this constitute a valid new offer?

18 Contract Law of the People's Republic of China, 1999. Available at: http://www.law-bridge.net/english/LAW/20064/0222320014345.html (last accessed 30 June 2013).

19 C. H. Ramberg (2001) 'The E-commerce Directive and formation of contract in a comparative perspective', *Global Jurist Advances*, 1 (2): Article 3.

In traditional contract law, once the offer is sent, it can be withdrawn if the withdrawal reaches the offeree before or at the same time as the offer even if it is irrevocable,[20] or the revocation of the offer reaches the offeree before he has dispatched an acceptance unless the offer is irrevocable.[21] In the electronic environment, the CISG Advisory Council Opinion 1 offers the interpretation that:

> The term 'reaches' corresponds to the point in time when an electronic communication has entered the offeree's server. An offer, even if it is irrevocable, can be withdrawn if the withdrawal enters the offeree's server before or at the same time as the offer reaches the offeree. A prerequisite for withdrawal by electronic communication is that the offeree has consented, expressly or impliedly, to receive electronic communications of that type, in that format and to that address.[22]

In contrast, the UN Convention provides a more specific rule on the notification duties and timing. It stipulates that 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.[23] 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.[24] 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,

20 CISG, Article 15(2).
21 CISG, Article 16.
22 CISG-AC Opinion no. 1, Electronic Communications under CISG, 15 August 2003. Rapporteur: Professor Christina Ramberg, Gothenburg, Sweden.
23 The UN Convention 2005, Article 14.
24 A/CN.9/546, pp. 102–3.

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.[25] 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.[26] It is notable that the principle of 'rights of withdrawal' has been included in international, regional and national legislation which can be employed to supplement the UN Convention to protect the right of the party online, in particular when the party has unintentionally hit a wrong key or web button and sent a message that he/she did not intend to send.

5.2 Example of the practical implications: Microsoft Outlook functions

There is an interesting functional tool 'recall or replace a message you've already sent'[27] in the Microsoft Outlook software which might also reveal some trends on the conditions of withdrawal or amendment of error in electronic communications.

It is noticeable that using the 'recall or replace a message' online sometimes can be easier and quicker than in the offline situation. However, this function has some restriction in that senders and recipients must all have Microsoft Exchange Server e-mail accounts to be able to use this tool. That is, senders can recall or replace a message if its recipient is logged on and using Microsoft Outlook. If the recipient has not read the original message or moved it from their Inbox, the original message will be deleted and replaced with the new message. If the recipient has read the original message or has saved it in a different folder, both the original message and new message will be available to the recipient. There is concern that whether the 'recall or replace a message' function can comply with the rule of 'error in electronic communications'.

In order to recall a message using the Microsoft Message Tool, the users should:

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

25 C. K. Wei and J. C. Suling (2006) 'United Nations Convention on the Use of Electronic Communications in International Contracts – a new global standard', *Singapore Academy of Law Journal*, 18: 116–202, at p. 162.

26 Explanatory Note 2007, p. 77 (Sales No. E.07.V.2).

27 Microsoft Outlook, 'Recall or replace a message you've already sent'. Available at: http://office.microsoft.com/en-001/outlook-help/recall-or-replace-an-email-message-after-it-is-sent-HA102749462.aspx?CTT=1 (last accessed 30 June 2013). There are similar features in Microsoft Exchange Server 2000, 2003, 2007, 2010 and 2013.

Next, users can choose one of the following actions:

1. *Recall the message*: Click 'Delete' unread copies of this message and select the 'Tell me if recall succeeds or fails' for each recipient checkbox 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 checkbox 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.[28]

There are two drawbacks to the above function of recall and replacement.

Firstly, the technique and functionality is restrictive, because the feature can only be used if your e-mails are handled by a Microsoft Exchange Server, which is a server that picks up the e-mails for the whole company and then passes them to the right client. So, users can't use this feature with a home PC which connects to someone's personal e-mail provider directly. Also this function is not available on Microsoft Outlook Web Access. Some software developers have developed various add-on services to remove some of the technical constraints on Microsoft Outlook. For example, WinDeveloper Message Recall v2.0 was introduced by WinDeveloper Software in 2012 as an add-on service to the Microsoft Recall Message functionality. It adds a server-side recalling process, bringing message recalling technology to the MS Exchange Outlook Web Access interface and working for both local and foreign recipients. If the recall action is taken within a few seconds, it is likely that the recipients will never see the original e-mail.[29]

Secondly, 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 that 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 is 'as soon as possible' itself.

In the absence of any time restriction on the message recall mechanism in Microsoft Outlook, the principle of 'the intentions of the parties' regarding the correction of input data should be deemed to be a criterion to determine whether the recalling or replacing of a message is done in good faith. This is

28 Ibid.

29 More information is available at: http://www.windeveloper.com/recall/recall_features.htm (last accessed 30 June 2013).

indicated by the leading case *Brinkibon Ltd* v. *Stahag Stahl and Stahlwarenhandel GmbH* which states:

> There may be 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.[30]

In addition, there are two possible legal effects in recalling and replacing an e-mail. 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 an 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.[31] 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'.[32] However, it is noted that Article 14 only applies to 'input errors', that is errors relating to inputting the wrong data, where the 'automated message system does not provide the person with an opportunity to correct the error', and not the other kinds of error such as a misunderstanding or misinterpretation of the terms of the contract.[33]

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 a scenario in which the seller A notices and corrects a price error before the order is 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 the two parties to communicate and

30 *Brinkibon Ltd* v. *Stahag Stahl and Stahlwarenhandel GmbH* [1982] 1 All ER 293.

31 C. K. Wei and J. C. Suling (2006) 'United Nations Convention on the Use of Electronic Communications in International Contracts – a new global standard', *Singapore Academy of Law Journal*, 18: 116–201, at pp. 162–3.

32 Ibid., p.163.

33 A/CN.9/546, pp. 188–90.

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.[34]

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 where the seller A delays notifying 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.

5.3 Example of regulatory harmonisation: European contract law

According to the current legislation, there are no clauses interpreting how parties' interests are balanced and at what level a reasonable time bar for notification of an electronic error should be set. How to define 'as soon as possible after having learned of the error' in the UN Convention and EC Directive on Electronic Commerce has been one of the most complicated issues. 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/she 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. 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 also in harmony with other needs that businesses and consumers may have due to the increased use of electronic communication.[35] The report covers six issues: 'input errors', 'cooling off periods', 'unsolicited contracts', 'definitions

34 C. Gringras (2003) *Laws of the Internet*, 2nd edn (London: Butterworths), p. 28.

35 Report from the Commission First Annual Progress Report on European Contract Law and the Acquis Review (hereafter 'PECL Report (2005)'), COM (2005) 456 final, Brussels, 23.09.2005, p. 4.

of sent, received and dispatched', 'definition of writing' and 'definition of signature'.[36] In this section, focus will lie 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 there is no need to change. But changes have been suggested to Article 4:104, as follows:

- An inaccuracy in the expression or transmission of a statement is to be treated as a mistake by the person who made or sent the statement and Article 4:103 applies.
- 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.
- The parties cannot derogate from paragraph (2) to the detriment of a consumer.[37]

Similar to that in the EC Directive and UN Convention, the above provision specifies the effects of errors occurring at a website and imposes a duty on online vendors to provide effective, accessible and technological means to the buyers to identify and correct input errors. As discussed earlier, it is clear that neither the EC Directive nor the UN Convention defines the time period for the correction of input errors. The PECL report fills the gap by suggesting 'cooling off periods (right to withdraw)' in detail.[38] 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.[39]

The efforts of the PECL report made to unify contracts concluded online are to be welcomed, regardless of whether the PECL electronic contract project

36 PECL Report (2005), p. 2.
37 PECL Report (2005), p. 8.
38 PECL Report (2005), p. 9.
39 PECL Report (2005), p. 17.

can eventually succeed. The two uniform principles of 'input errors' and 'the time period to withdraw' in the report should be highly recommended for electronic commercial transactions at the international level. The EC Directive on Consumer Rights 2011 (Article 9(1)) introduces identical conditions for a 14-day cooling off period in which 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, the uniform time period for 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 only when the contract is concluded, and also 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.

6 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] With the deployment of cloud computing services, customers and users may not be able to choose or restrict the location of data centres prior to the conclusion of the Service Level Agreement (SLA). Data centres may be relocated or added at any time and as a result they may be located in various jurisdictions which could contribute to the difficulty in identifying the location of infringement and determining the competent court and applicable law.[2]

A great success of the Internet is the creation of a worldwide marketplace. It is noticeable that there has been a significant increase in the number of cross-border transactions since the usage of the Internet. Thus a trader in Rome can, through a web page, reach a customer in New York just as easily as one in Sorrento, or in a multiple establishment, A's head office is in the UK, but a team based in China handles technical control of the website, while customer support and credit card processing is conducted in the USA and cloud data centres are located in Asia Pacific. So where is the company established? This cross-border impact 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.[3] 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

1 C. Gringras (2003) *Laws of the Internet*, 2nd edn (London: Butterworths), p. 16.

2 F. Wang (2012) 'IP and cloud computing: the progress of a digital agenda for Europe', *Intellectual Property Forum*, 89: 92–4, at p. 93.

3 A. D. Murray (2000) 'Entering into contracts electronically: the real WWW', in L. Edwards and C. Waelde (eds), *Law and the Internet: A Framework for Electronic Commerce* (Oxford: Hart), pp. 17–35.

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.[4]

Due to the complexity of Internet jurisdiction and choice of law, the trader may prefer to enter into contracts with certain parties from the local region rather than any country, thus 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.

6.1 Place of business

In addressing this issue, the Model Law on Electronic Commerce (Article 15) sets out a series of 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.[5] 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.[6]

The UN Convention further provides the determination of the location of the parties (Article 6). This provision can be helpful in determining jurisdiction, applicable law and enforcement. Its aim is to remove legal obstacles to cross-border electronic commerce. It clearly explicates the definitions 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 that 'maintains a non-transitory establishment to pursue an economic activity other than the temporary provision of goods or services out of a specific location',[7] 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.[8] 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.[9] 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

4 I. Lloyd (2000) *Legal Aspects of the Information Society* (London, Edinburgh and Dublin: Butterworths), p. 243.
5 UNCITRAL Model Law on Electronic Commerce, Article 4(a).
6 UNCITRAL Model Law on Electronic Commerce, Article 4(b).
7 The UN Convention 2005, Article 4(h).
8 The UN Convention 2005, Article 6(1).
9 The UN Convention 2005, Article 6(2).

is not merely the place where the equipment and technology are located or a domain name is registered.[10]

In the EU, the EC Directive on Electronic Commerce (Recital 19) uses the benchmark of 'economic activity' to determine the establishment/place of a service provider, provided that:

> the place at which a service provider is established should be determined in conformity with the case law of the Court of Justice according to which the concept of establishment involves the actual pursuit of an *economic activity* through a fixed establishment for an indefinite period; this requirement is also fulfilled where a company is constituted for a given period.

Recital 19 further confirms that:

> The place of establishment of a company providing services via an Internet website is not the place at which the technology supporting its website is located or the place at which its website is accessible but the place where it pursues its *economic activity*; in cases where a provider has several places of establishment it is important to determine from which place of establishment the service concerned is provided; in cases where it is difficult to determine from which of several places of establishment a given service is provided, this is the place where the provider has the centre of his activities relating to this particular service.[11]

The EC Distance Selling Directive (Article 5(1)) does not provide rules on the determination of the place of business but requires 'the geographical address of the place of business of the supplier to which the consumer may address any complaints'.[12] The EC Directive on Consumer Rights 2011 (which comes into force in 2014) explicitly requires the information provided for the geographical address at which the trader is established.[13]

In the US, the UCITA (Section 109(d)) 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.'[14] The UETA (Section 15(d))

10 The UN Convention 2005, Article 6(4) and (5).
11 EC Directive on Electronic Commerce 2000, Recital 19.
12 EC Distance Selling Directive 1997, Article 5(1).
13 EC Directive on Consumer Rights 2011, Article 6(1).
14 UCITA, Section 109(d).

specifies a more specific rule which is similar to the wording in the UN Convention that:

> (1) if the sender or recipient has more than one place of business, the place of business of that person is the place having *the closest relationship* to the underlying transaction; and
> (2) if the sender or the recipient does not have a place of business, the place of business is *the sender's or recipient's residence*, as the case may be.[15]

In China, the Chinese Electronic Signatures Law (Article 12) deals with the main place of business of the sender and the recipient. It states that the place where the data message is sent or received 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. This is consistent with the general rule in the China Contract Law. The China Contract Law provides a relevant provision dealing with the place of formation concerning electronic messages. It provides that:

> The place where the acceptance becomes effective is the place of formation of a contract. Where a contract is concluded by the exchange of electronic messages, *the recipient's main place of business* is the place of formation of the contract; if the recipient does not have a main place of business, its *habitual residence* is the place of formation of the contract. If the parties have agreed otherwise, such agreement prevails.[16]

That is, in general the China Contract Law promotes party autonomy and indicates the main linking factors in determining the place of the formation of the contract: the recipient's main place of business and habitual residence.

6.2 Place of performance

Place of performance is another important criteria of determining jurisdiction and applicable law when disputes occur. It can be linked with the '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 following:

> 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

15 UETA, Section 15(d).
16 China Contract Law 1999, Article 34.

at the place where the addressee has its place of business, as determined in accordance with article 6.

In the EU, in the old version of the Principles of European Contract Law 1995, Article 2.106 of the PECL (1995) 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.

It is noticeable that the place of business and habitual residence are the main factors in determining the place of performance in the old PECL. There are similar rules under the Rome I Regulation 2008. For example, the Rome I Regulation (Article 4(2)) specifies that where the contract is not covered by Article 4(1) or where the elements of the contract would be covered by more than one of points (a) to (h) in Article 4(1), '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'.[17] Compared with the Rome I Regulation, the Brussels I Regulation 2000 (and 'the Brussels I Recast') provides much more explicit wording in the clarification of the place of performance of the obligation than in the case of the sale of goods which is 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.[18] The place of delivery and place of services provided

17 Council Regulation (EC) No. 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), OJ L 177/6 – 16, 04.07.2008. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:177:0006:0016:EN:PDF (last accessed 30 June 2013), Article 4(2).

18 Council Regulation (EC) No. 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, OJ L12/1-22, 16.01.2001. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:012:0001:0023:EN:PDF (last accessed 30 June 2013), Article 5(1)(b); and the Regulation (EU) No. 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast). Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:351:0001:0032:En:PDF (last accessed 30 June 2013).

are the performing factors. In the US, concepts such as 'minimum contacts',[19] 'effects'[20] and 'targeting tests'[21] are used to determine the place of performance. In China, there are similar approaches to determine the place of performance subject to national law. For example, the China Contract Law (Article 63(3)) provides that:

> Where the place of performance was not clearly prescribed, if the obligation is payment of money, performance shall be at the place where the payee is located; if the obligation is delivery of immovable property, performance shall be at the place where the immovable property is located; for any other subject matter, performance shall be at the place where the obligor is located.[22]

In general, principles such as party autonomy and connecting factors have been employed to determine the place of performance in the Chinese Civil Procedure Law.[23]

The 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. More detail will be discussed in Part IV.

19 *Zippo Manufacturing Co.* v. *Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W.D. Pa. 1997).
20 *Calder* v. *Jones*, 465 US 783 (1984).
21 952 F. Supp. 1119 (W.D. Pa. 1997).
22 China Contract Law, Article 63(3).
23 Chinese Civil Procedure Law, Articles 25 and 243.

7 Contemporary issue: the electronic battle of the forms

Businesses generally wish to contract using their own standard conditions because they may have drafted their contracts to meet their own product, service, project, technical, commercial and legal requirements.[1] The result is called a 'standard contract'. Standard terms are contract terms that one party formulates for use in their contracts generally and are provided 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 principle subject matter. Standard terms or general terms are often referred to pejoratively as 'boilerplate'.[2] The boilerplate terms[3] sometimes 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. In some situations, it is possible that standard terms designed for use in one country are subject to laws for which they are not designed.[4] This may cause trouble for enforcement.

One of the most crucial issues here is 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 are the terms of the contract. This is the so-called 'battle of the forms'. It arises where two companies are in negotiation and as part of their exchanges they each send standard contract forms but the two sets of forms are incompatible.[5] That is, a battle of the forms arises when each party

1 D. W. Bartell (2000) *E-contracts* (Ledbury: BWCS Ltd), p. 208.
2 J. R. Maxeiner (2003) 'Standard-terms contracting in the global electronic age: European alternatives', *Yale Journal of International Law*, 28 (1): 110.
3 'Boilerplate' means general conditions while 'front-form' refers to essential or important conditions.
4 J. R. Maxeiner (2003) 'Standard-terms contracting in the global electronic age: European alternatives', *Yale Journal of International Law*, 28 (1): 111.
5 R. Stone (2005) *The Modern Law of Contract*, 6th edn (London: Cavendish), p. 41.

has their own standard terms of trading or business that they want to prevail over the other party's standard terms.[6]

The 'battle of the forms' is one of the controversial issues in traditional contract law due to the divergent treatment within and among different jurisdictions. It is noteworthy to take the British common law system as an example. In an leading English 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 the forms: first, whether there is an expressed term or implied term from the conduct with regard to 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 while 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. That is, 'he did not apply the traditional method of analysis by way of offer and counter-offer.'[9] Instead, he preferred to examine whether there is an agreement on material points, and if there is, to determine the agreed and conflicted terms.[10] 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'.[11] In the more recent case of *Tekdata Interconnections Ltd* v. *Amphenol Ltd*, the Court of Appeal looked into the business relationship in terms of the course of dealing between the buyer (Tekdata) and the seller (Amphenol) but applied the traditional offer and acceptance analysis that Amphenol's acknowledgment of the order with Amphenol's terms were to apply (the 'last-shot' doctrine).[12]

6 A. D. M. Forte (2006) 'The battle of forms', in H. L. MacQueen and R. Zimmermann (ed.), *European Contract Law: Scots and South African Perspectives* (Edinburgh: Edinburgh University), pp. 98–122, at p. 98.

7 *Butler Machine Tool Co. Ltd* v. *Ex-Cell-O Corpn (England) Ltd* [1977] EWCA Civ. 9; [1979] WLR 401; [1979] 1 WLR 401.

8 [1979] 1 WLR 401, pp. 404–5; see also R. Rawlings (1979) 'The battle of the forms', *Modern Law Review*, 42: 715–21, at pp. 716–17.

9 *Butler Machine Tool Co. Ltd* v. *Ex-Cell-O Corpn (England) Ltd* [1977] EWCA Civ. 9; [1979] WLR 401; [1979] 1 WLR 401.

10 A. D. M. Forte (2006) 'The battle of forms', in H. L. MacQueen and R. Zimmermann (ed.), *European Contract Law: Scots and South African Perspectives* (Edinburgh: Edinburgh University), pp. 98–122, at p. 101.

11 Ibid., p. 102.

12 *Tekdata Interconnections Ltd* v. *Amphenol Ltd* [2009] EWCA Civ. 1209; [2009] 2 CLC 866; [2010] 1 Lloyd's Rep 357.

Lord Justice Longmore said 'it will always be difficult to displace the traditional analysis, in a battle of forms case, unless it can be said there was a clear course of dealing between the parties. That was never proved.'[13] He accepted that the *Butler* case was not a precedent for abandoning the traditional analysis.[14] In contrast, in the most recent Scottish case of *Specialist Insulation Ltd* v. *Pro-Duct (Fife) Ltd*, express acceptance was not signed by Pro-Duct (Fife) Ltd and was not returned to the supplier.[15] The court considered that 'as stressed in *Tekdata*, the subjective intentions or beliefs of the parties give way to an objective interpretation of their communications when viewed in the context of the circumstances of the case. Thus an absence of consensus, even on an important issue, need not prevent the court from deciding that there is a contract and then resolving its terms.'[16] The court confirmed that there was a contract; however, it did not apply the 'last-shot' doctrine to determine whether the adjudication clause was included. It ruled that the adjudication clause never formed part of the agreement as there was no intention to create any new obligations either express or implied.[17] It is obvious that different approaches have been taken in the British common law system, based on the circumstances.

National, regional and international legislative instruments have tried to harmonise the 'battle of the forms' rule in contracts in order to increase predictability and legal certainty. 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 (hereafter 'UNIDROIT Principles') and the Principles of European Contract Law (PECL) have proposed rules for the 'battle of the forms' but inevitably these have led to different outcomes in some circumstances.[18] However, the legislation examples have something in common in that they follow a 'two-stage' process: the first stage is to determine whether there is a contract existing between the parties, and the second stage is to ascertain it by finding whether the exchanged terms materially differ and what terms prevail.[19]

13 [2009] EWCA Civ. 1209, para. 21.
14 [2009] EWCA Civ. 1209, para. 10.
15 *Specialist Insulation Ltd v. Pro-Duct (Fife) Ltd* [2012] CSOH 79, para. 22.
16 [2012] CSOH 79, para. 23.
17 [2012] CSOH 79, para. 40
18 K. C. Stemp (2005–6) 'A comparative analysis of the 'battle of the forms', *Transnational Law and Contemporary Problems*, 15: 244.
19 A. D. M. Forte (2006) 'The battle of forms', in H. L. MacQueen and R. Zimmermann (ed.), *European Contract Law: Scots and South African Perspectives* (Edinburgh: Edinburgh University), pp. 98–122, at p. 102.

7.1 International legislation: CISG and the UNIDROIT Principles

Article 19 of the CISG provides that a reply to an offer that contains additions, limitations or other modifications constitutes a counter-offer.[20] 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.

Article 19(1) of the CISG is considered to be the 'mirror-image' rule that if a reply to the offer contains materially different terms as to additions, limitations or other modification of the original offer it should be treated as a rejection of the original offer and constitutes a counter-offer. For example, in the *Oberlandesgericht Frankfurt am Main (Germany) Shoes* case, the Court of Appeal confirmed the judgment in the Court of First Instance that there was no contract as the buyer's order constituted a counter-offer as it contained different quantities and the price of some ordered items was neither fixed nor determinable.[21] It is consistent with the 'mirror-image' rule in CISG, Article 19(1), because if the buyer's order reflected the terms in the seller's invoice, it would have been a valid acceptance.

Article 19(2) of the CISG further provides that the reply purports to be an acceptance, and additional and different terms prevail over the terms of offer, if they do not materially differ those terms of offer, though the offeror has the right to object any immaterial changes without undue delay. If the offeree's reply is the last document to change hands before performance, its terms will bind the parties.[22]

An overall interpretation of the materiality of the terms is given by Article 19(3) of the CISG. It provides a non-exhaustive list of matters which are in theory of materiality. Although the determination may not be so

20 United Nations Convention on Contracts for the International Sale of Goods (CISG), U.N. Doc. A/COF. 97/18 (Apr. 11, 1980). 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.

21 Oberlandesgericht Frankfurt am Main, 10. Zivilsenat (Shoes case) 04.03.1994, 10 U 80/93, CISG-online 110. Available at: http://www.globalsaleslaw.org (last accessed 30 June 2013).

22 K. C. Stemp (2005–6) 'A comparative analysis of the 'battle of the forms', *Transnational Law and Contemporary Problems*, 15: 261.

straightforward, it provides some useful guidelines for reference. The success of the CISG lies in the interpretation of materially altering terms.

It is notable that Article 19 of the CISG together with Article 7 also employ the 'knock-out' rule with regard to conflicting terms and retaining those in common (non-materially different) in general terms and conditions. For example, in the Bundesgerichtshof (Germany) *Powdered Milk* case,[23] the Court of Appeal confirmed that 'the partial contradiction of the referenced general terms and conditions of [buyer 1] and [seller 1] did not lead to the failure of the contract within the meaning of Article 19(1) and (3) CISG because of the lack of a consensus (dissent).' It further asserted that 'according to the (probably) prevailing opinion, partially diverging general terms and conditions become an integral part of a contract (only) insofar as they do not contradict each other.' It is suggested that in practice, courts are inclined to apply Article 19 of the CISG for the incorporation of terms and conditions in the battle of the forms and both the 'last-shot' and 'knock-out' rules are equally present in determining the terms of the contract, though it is agreed that the 'knock-out' rule gives a more favourable solution to the battle of the forms as it allows a degree of flexibility corresponding to the parties' intent.[24]

In contrast, the UNIDROIT Principles (Article 2.1.22) explicitly present a provision on the battle of the forms and adopt a 'knock-out' rule. They provide that:

> 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]

This is generally considered an attempt to provide a solution to the CISG non-specific rule on the battle of the forms.

7.2 US legislation: UCC

Unlike the CISG that will still allow an offeror to reject an acceptance that contains immaterial variations, the UCC Section 2–207, similar to the UNIDROIT Principles, will find the existence of a contract as long as the major terms

23 *Bundesgerichtshof* (Federal Supreme Court) 09.01.2002, VIII ZR 304/00, Germany (Powdered milk case). Available at: http://cisgw3.law.pace.edu/cases/020109g1.html (last accessed 30 June 2013).

24 A. Fejōs (2006) *Formation of Contracts in International Transactions: The Issue of Battle of the Forms under the CISG and the UCC.* Available at: http://www.cisg.law.pace.edu/cisg/biblio/fejos.html (last accessed 30 June 2013).

25 UNIDROIT Principles of International Commercial Contracts 2010, Article 2.1.22.

match.[26] However, the CISG does not address the question of what happens when conflicting offers and acceptances are exchanged and performance nonetheless begins, whereas Section 2–207(3) of the UCC provides some reference.[27]

Section 2–207 of UCC[28] 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 the battle of the forms is far from 'uniform'. While Section 2–207(1) refers to 'additional or different terms', Section 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.'[29] The Cambridge Online Dictionary defines 'different' as 'not the same' while explaining 'additional' as 'extra'.[30] The word 'different' is defined as 'not the same as another or each other' or 'distinct and separate', while it describes 'additional' as 'added, extra, or supplementary' in the Compact Oxford Online English Dictionary.[31] 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

26 K. C. Stemp (2005–6) 'A comparative analysis of the 'battle of the forms', *Transnational Law and Contemporary Problems*, 15: 261.

27 L. F. Del Duca (2005) 'Implementation of contract formation statute of frauds, parol evidence, and battle of forms CISG provisions in civil and common law countries', *Journal of Law and Commerce*, 25: 133.

28 UCC Section 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 through 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:
>
> a. the offer expressly limits acceptance to the terms of the offer;
> b. they materially alter it; or
> c. 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 recognizes 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.

29 Article 2–207(2) of UCC.

30 Available at: http://dictionary.cambridge.org (last accessed 30 June 2013).

31 Available at: http://oxforddictionaries.com (last accessed 30 June 2013).

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') has the same effect on the contract: it makes the contract look different.

Section 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. Section 2–207(2) accepts that additional terms may become part of the contract except for offer limitations, material alterations or advanced notifications. Section 2–207(3) applies to 'where documentary exchanges between parties do not disclose a concluded contract'.[32] Under Section 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, while the other conflicting terms are left out, and the other provisions of the UCC are supplemented.[33]

7.3 EU legislation: PECL

Differing from the UCC and the CISG, the UNIDROIT Principles and PECL separate and treat conflicts of general conditions differently from essential terms.[34] The UNIDROIT Principles (Articles 2.1.11 and 2.1.22),[35]

32 A. D. M. Forte (2006) 'The battle of forms', in H. L. MacQueen and R. Zimmermann (ed.), *European Contract Law: Scots and South African Perspectives* (Edinburgh: Edinburgh University Press), pp. 98–122, at p. 113.

33 C. Torre and G. Allen (2006) 'The battle of the forms – there is a purpose', *Journal of Legal Studies Education*, 23 (2): 195–216, at pp. 202–9.

34 J. E. Murray (2000) 'The definitive "battle of the forms": chaos revisited', *Journal of Law and Commerce*, 20: 41.

35 UNIDROIT Principles of International Commercial Contracts (1994), 34 ILM 1067 (1995), available at: http://www.unidroit.org/english/principles/contracts/principles1994/fulltext.pdf (last accessed 30 June 2013). 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.

as do the PECL (Articles 2:208 and 2:209),[36] 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 UNIDROIT Principles and the PECL are consistent with the CISG in 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 UNIDROIT 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'.[37]

The UNIDROIT Principles and PECL attempt to offer both the efficiency and practicality of the CISG 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

36 The Principle 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.

Article 2:209 of the PECL 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 substance.
> (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.

37 A. D. M. Forte (2006) 'The battle of forms', in H. L. MacQueen and R. Zimmermann, (ed.), *European Contract Law: Scots and South African Perspectives* (Edinburgh: Edinburgh University), pp. 98–122, at p. 117.

when differing terms are likely to go unnoticed.[38] The outcomes of conflicting general conditions are the same referring to the UNIDROIT Principles (Article 2.1.22) and the PECL (Article 2:209). The contract is nonetheless formed because both the UNIDROIT Principles (Article 2.1.22) and the PECL (Article 2:209) 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, the CISG, the UNIDROIT Principles and the PECL have their 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 the issue of whether a valid contract exists despite the existence of conflicting terms and what terms will apply. The CISG, the UNIDROIT Principles and the 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 discussed earlier, they distinguish the situations between essential terms and general conditions.

7.4 Chinese legislation: China Contract Law

The Contract Law of the People's Republic of China (hereafter the 'China Contract Law') strongly encourages the usage of standard term contracts. The provisions regulating standard terms are specified in the China Contract Law, Articles 39 to 41. 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.[39] Article 41 continues the protection of the parties who are supplied with standard terms that 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 the battle of the forms is governed by the China Contract Law but without specific provisions directly referring to the electronic battle of the forms. The basic provision of the 'battle of the forms' in China

38 K. C. Stemp (2005–6) 'A comparative analysis of the "battle of the forms"', *Transnational Law and Contemporary Problems*, 15: 266.

39 China Contract Law, Article 40.

Contract Law (Article 20) sets four conditions regarding the revocation of an offer, which affirm the importance of the effect of material terms in an acceptance of the offer. That is, an offer shall be revoked 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.

It is obvious that this rule is identical to Article 19(1) and (3) of the CISG, though the different wording of 'substantial changes' in the context in Article 20(4) should be understood as 'material addition, alternations and modifications'.

In addition to Article 20, Articles 30 and 31of the China Contract Law gives more precise details on the validity of substantial changes to offer and acceptance, which are arguably provisions governing the materiality of terms in the battle of the forms. This is identical to the 'mirror-image' rule. Article 30 of the China Contract Law governs the 'acceptance containing material change', which provides:

> The terms of the acceptance shall be identical to those of the offer. A purported acceptance dispatched by the offeree which materially alters the terms of the offer constitutes a new offer. A change in the subject matter, quantity, quality, price or remuneration, time, place and method of performance, liabilities for breach of contract or method of dispute resolution is a material change to the terms of the offer.

It 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.[40] Furthermore, Article 31 specifies the 'acceptance containing non-material changes', which provides:

> An acceptance containing nonmaterial changes to the terms of the offer is nevertheless valid and the terms thereof prevail as the terms of the contract, unless the offeror timely objects to such changes or the offer indicated that acceptance may not contain any change to the terms thereof.

That is, 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. This is identical to the 'knock-out' rule in the UNIDROIT Principles.

40 China Contract Law, Article 30.

In short, it is noticeable that the China Contract Law adopts the 'mirror-image' and 'knock-out' rules for the regulation of the battle of the forms. It also provides a concept that is equivalent to 'material alterations', which is that 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.[41] This is compatible with the UCC, the CISG, the UNIDROIT Principles and the PECL in that material alterations of an offer are a rejection of an offer and constitute a counter-offer.

7.5 Proposed solutions to the electronic battle of the forms

It may be even more challenging to amalgamate the 'mirror-image', 'last-shot' and 'knock-out' rules of the battle of the forms and apply them in an electronic environment. An electronic battle of forms will demand additional consideration of the features of instantaneous electronic communications. It is likely that in an electronic battle of the forms the interpretation of traditional rules may need to intertwine with the concepts of dispatch and receipt of an electronic communication,[42] the validity of offer and acceptance by electronic means, the availability of contract terms by electronic means,[43] the incorporation of terms and conditions by electronic means, and error in electronic communications.[44]

There are at least three prerequisites for the determination of which form should prevail and which battle should win in an electronic contracting environment. The first prerequisite is the appropriate and effective manner of making contractual terms available in electronic form. The existence or modification of the terms should be brought to the attention of customers before they can give an informed consent. Terms displayed in an electronic form should be able to be stored and printed for later reference. In some regions such as the EU, the terms and conditions will be valid in a durable medium between the seller and the consumer.

The second prerequisite is the appropriate technical measures provided for correcting an input error in electronic communications. Error in electronic communications should be amended without undue delay and within a reasonable timeframe. Legal principles such as fairness and transparency and appropriate measures such as technical and enforcement measures should be employed to prevent unfair conduct in electronic contracting, taking into account the speed of an electronic communication.

41 China Contract Law, Article 30.
42 The UN Convention 2005, Article 15(1).
43 The UN Convention 2005, Article 13.
44 The UN Convention 2005, Article 14.

The third prerequisite is the intention of the parties to form a contract by electronic means, not merely communicating an enquiry by electronic means. On an e-commerce platform, terms and conditions of sale and service are often presented to the buyer in standard forms. In an automated transaction system, customers should be alerted to the consequences of pressing the 'I agree' button, for example, by means of a clear warning message stating 'terms and conditions presented will be binding once the order is submitted'. In e-mail communications, it is also recommended to have a clear wording as to the intention of forming contractual terms to avoid later disputes, though in some circumstance it might be possible to detect the intention by reviewing all messages as a whole.

The disputes in an electronic battle of the forms are likely to happen in a situation in which two trading companies (the Seller 'A' and the Buyer 'B') both have their own standard terms of sale and purchase with collision terms, exchanging their terms by electronic means. For example, suppose 'B' ordered products from 'A' by submitting a purchase order form by e-mail indicating that the buyer's terms will prevail over the seller's standard terms and attaching the buyer's standard terms of purchase. This usually constitutes a counter-offer, though it should be distinguished from a situation in which the responding party is merely requesting information. For example, in the leading English case of *Stevenson* v. *McLean* [1879–80], the defendants offered to sell a quantity of steel to the plaintiffs at 40s. per ton. The plaintiffs responded by enquiring as to whether the defendants would accept 40s. for delivery over two months, or if not, what the longest time was that they would give. It was held that the plaintiffs constituted a request for information, because the plaintiffs were not seeking to introduce new terms into the offer, but requesting the clarification of the existing terms. The offer of 40s. per ton was therefore still open to acceptance.[45] If the buyer is not merely requesting information and the seller is not willing to accept the buyer's full standard terms of purchase by simply confirming a 'yes' in return, the battle of the forms may immediately start. If the seller responds to the buyer by e-mailing an acknowledgment form making additions, alterations or modifications of the buyer's essential terms which are of material difference, it may revoke the purchase offer in a purchase order form. If the additional, alterative or modified terms are not materially different from the buyer's standard terms of purchase, a contract of sale may nevertheless be formed with the buyer's standard terms of purchase with non-material modifications but knocking out conflicted general terms, provided that the buyer does not reject it without undue delay. In some countries such as China, it requires a final confirmation of letter executing a contract by the exchange of letters or electronic messages to enhance the certainty as to when the contract is finally formed.[46] In the EU, the proposed electronic timing

45 *Stevenson* v. *McLean* [1879–80] LR 5 QB 346.
46 China Contract Law, Article 33.

stamp and electronic delivery services in a proposal of the Regulation on 'Electronic Identification and Trusted Services for Electronic Transactions in the Internal Market'[47] may further assist in defining the effectiveness of an electronic battle of the forms.

It is notable that the harmonisation of the determination of an electronic battle of the forms will be beneficial to enhance the legal certainty and fairness for cross-border commercial transactions. This may be achieved by the amalgamation of the traditional 'battle of the forms' rules in the international legislation (such as the CISG and UNIDROIT Principles) and the modern 'electronic communications' rules in the UN Convention on the Use of Electronic Communications in International Contracts or other relevant regional and national laws in practice. It is evitable that an electronic acceptance that contains additions, limitations or other modifications may be a rejection of the offer and constitute a counter-offer. 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 as parties otherwise agree. This should apply where parties have met the three prerequisites for forming a contract in an electronic contracting environment.

47 COM (2012) 238 final.

Part II 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 will be either to 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 in the law because their implementation is on a voluntary basis, while the tradition of not stipulating the sanctions and effects results in the directives being implemented differently in each of the Member States.[48] By contrast, the development of international model laws and conventions governing the issues regarding electronic commercial transactions provides standardisation and gap-filling measures by setting core technology-neutral principles to promote harmonisation at the international level. There has also been an ongoing debate over the possible design of establishing an optimised legal infrastructure for global electronic commercial transactions, such as by stimulating the interplay among hard law, self-regulation, best practices and co-regulation.

Nevertheless, national laws have been providing a solid foundation in regulating the national e-commerce markets. In the EU, US and China, the EC Directive on Electronic Commerce and EC Distance Selling Directive (replaced by the EC Directive on Consumer Rights 2011), the US Uniform Electronic Transaction Act (UETA) and the China Electronic Signatures Law have been well implemented in the information society. 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 progress in modernising, standardising and harmonising electronic communications in international contracts. They have in common that they employ the principle of functional equivalency for a record or signature in an electronic form. It is notable that the EC Directive on Electronic Commerce is different in that it particularly requires that 'the service provider has to acknowledge the receipt of the recipient's order without undue delay and by electronic means'.[49] It was argued that there is 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.[50] In the author's view, the ruling of confirmation of the receipt of the recipient's

48 C. H. Ramberg (2001) 'The E-commerce Directive and formation of contract in a comparative perspective', *Global Jurist Advances*, 1 (2): 25.

49 EC Directive on Electronic Commerce, Article 11.

50 C. H. Ramberg (2001) 'The E-commerce Directive and formation of contract in a comparative perspective', *Global Jurist Advances*, 1 (2): 14.

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, acknowledgment of receipt is not equivalent to an acceptance, although it might perform a function as an acceptance in clickwrap agreements. The proposed electronic timing stamp and electronic delivery services in a proposal of the Regulation on 'Electronic Identification and Trusted Services for Electronic Transactions in the Internal Market'[51] may provide an example of best practices for the enhancement of the certainty of the effectiveness of an electronic communication.

While nations have been putting continuous efforts into revising and modernising their national legal instruments, international organisations have also been continuing their efforts. The UN Convention entered into force on 1 March 2013 after the text was adopted by UNCITRAL in 2005. Up until 2013, only 18 countries (including China but not the US or EU Member States) have signed the UN Convention and only three countries (Dominican Republic, Honduras and Singapore) have ratified it (Dominican Republic provided accession).[52]

Nonetheless, the UN Convention complementing the UNICTRAL Model laws on electronic commerce and electronic signatures has provided most nations with a good reference in terms of provisions and wording for the drafting of national law. The UN Convention serves as a model to enhance legal certainty and the 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, and automated transactions.[53] The UN Convention also harmonises 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', which can consider the combination of three concepts: 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

51 COM (2012) 238 final.

52 Status: 2005 – United Nations Convention on the Use of Electronic Communications in International Contracts, available at: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention_status.html (last accessed 30 June 2013).

53 The United Nations Convention on the Use of Electronic Communications in International Contracts (A/60/515).

contracting such as e-mailing from instantaneous contracting such as click-wrap agreements, because although contracting by e-mail is non-instantaneous, it is still much quicker than normal postal services. In addition, different e-mail servers and different Internet services can vary in speed in sending and receiving messages, thus some e-mails might almost be like instantaneous messages, so it would be more difficult to reach consensus and efficient harmonisation of the rule for different standard users and make it fair. Therefore it should be more sensible to apply the 'acceptance' or 'receipt' rule to electronic contracting.

Thirdly, the UN Convention lacks provisions regulating individual communications of e-contracts, which becomes a noteworthy issue in electronic transactions. With the increasing improvements in the IT industry and e-commerce services, online companies can offer the customer a lot 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 contentment.

Fourthly, technology-neutral measures and the interpretation of the timing 'as soon as possible after having learned of the error' should be considered for the revision of the provision on 'error in electronic communications'. This is to adapt to the ever-changing information society that more new functionality in electronic communications may be consistent with the existing wording of notifying other parties 'as soon as possible after having learned of the error' under the UN Convention. For example, the issue was discussed earlier regarding the 'recall or replace a message you've already sent' function in Microsoft Exchange Server.

Lastly, the UN Convention is silent on the 'battle of the forms' rule in electronic commercial transactions, which, in the author's view, it is necessary to include since it will occur more often when more and more large or medium-size firms get involved with cross-border online trading. As discussed earlier, the traditional rules contained in the UCC, the CISG, the UNIDROIT, the PECL and the China Contract Law should be combined to apply to the online battle of the forms, though the amalgamation of the traditional 'mirror-image', 'last-shot' and 'knock-out' rules should be subject to three prerequisites for the formation of electronic contracts.

Overall, nations have made efforts to expedite the development of electronic commerce and inevitably different approaches or methodologies have been adopted due to historical, social, cultural, economic and political differences. It is notable that the US is attempting to drive the international marketplace into the Internet age, while the EU approach initially appears to be more focused on growing the internal marketplace. Since 2010 the EU has been cooperating with many countries and international organisations to represent Europe's interests as one of the goals set in the Digital Agenda

for Europe.[54] In China, since the enactment of the Electronic Signatures Law, numerous notices and measures (local legal instruments) have been proposed and implemented to adapt to the development of the e-commerce markets. It is obvious that China, together with the rest of the international community, have been searching for a harmonious global solution, though the process of modernisation and harmonisation can be lengthy and arduous, involving the infusion of a prodigious amount of coordination, expertise, time and costs.

54 Digital Agenda for Europe, COM (2010) 245 final/2.

Part III
Online Security

This page intentionally left blank

8 Electronic signatures and electronic authentication

8.1 Electronic signatures

A handwritten signature is a familiar way for individuals to make apparent on paper-based documents that they are who they say they are and that, often, they agree to be bound by whatever they are signing. A handwritten signature, therefore, generally provides authentication of the signatory. It is also an indication of 'acceptance' or 'consent' to a legally binding commitment such as contractual terms or payment.[1]

An electronic signature, another form of signature which has emerged in modern society, has been considered an equivalent to traditional handwritten signatures or stamps.[2] In an electronic commercial transaction, electronic signatures have been used as a means to indicate the identity of the communicating parties and subsequently to protect data privacy and security in electronic commerce in open networks.

With the rapid development of new technologies, online security becomes more and more significant as security compromises are one of the major barriers to building users' trust in electronic commercial transactions. It is notable that the mutual recognition of electronic identification, authentication and electronic signatures plays a vital role in facilitating electronic transactions and in strengthening users' trust in them.[3] It is understandable that parties need to know that the sender of an electronic message is actually the person they claim to be. In addition, communicating parties also need to

1 *L'Estrange* v. *F. Graucob Ltd* [1934] 2 KB 394, a contract was formed by signature. *Central Motors (Birmingham) Ltd* v. *PA & SNP Wadsworth* [1982] CAT 231; [1983] 133 NLJ 555 – a signature on the cheque constituted an agreement to pay.

2 F. Wang (2010) *Law of Electronic Commercial Transactions: Contemporary Issues in the EU, US and China* (Oxford: Routledge), pp. 77–87.

3 Communication of a coherent framework to build trust in the digital single market for e-commerce and online services, European Commission, Brussels, 11.01.2012, COM (2011) 942 final, p. 9.

ensure that the electronic message has not been altered which may change the sender's original intention or meaning, i.e. the integrity of the message.[4]

In order to enhance their effectiveness, electronic signatures may also be qualified by certificates issued by certification service providers (CSPs). This is to certify the veracity of the link between the electronic signature and the identity of the electronic signature holder. With the increased use of smart devices and pace of globalisation, a trusted third party may be employed to further enhance users' confidence in an e-commerce website as in theory an electronic transaction can be made by users at any time without any territorial restriction. Private and public organisations, which provide an active and interactive online service, also have to keep updating appropriate technical and other measures to enhance security, prevent identity theft and protect the users' rights. If an e-commerce system was attacked, it could lead to service interruption or even loss of data. For example, in April 2013 there were distributed denial of service (DDoS) attacks which disrupted the availability of the Dutch Internet banking website, and more than 10 million Dutch citizens were unable to use their official online signature to pay bills and taxes because of a DDoS attack.[5]

There are various technical measures for security protection. It is notable that websites often use a technology called Secure Sockets Layer (SSL) to encrypt personal information over the Internet. Customers usually look for trustmark logos such as VeriSign or TRUSTe to increase their confidence in undertaking an electronic transaction on an e-commerce platform. It is obvious that, as a result of a technology shift from traditional face-to-face transactions, technical architectures and authentication measures often substitute for the trust that trading partners formerly developed between each other.[6] Identification and authentication provide 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.[7]

In response to the rapid digital market development by new technologies, nations and international organisations have been revising current legislation

4 F. Wang (2004) 'Another consideration about legal system of electronic authentication', *Forward Position in Economics*, 2–3: 105–8; see also R. Julia-Barcelo and T. C. Vinje (1998) 'Another step towards a European Framework for electronic signatures: the Commission's Directive Proposal', *Computer Law and Security Report*, 14 (5): 303.

5 'DDoS attack caused disruption of the availability of websites', Dutch National Cyber Security Centre (NCSC), Ministry of Security and Justice, 19 April 2013. Available at: https://www.ncsc.nl/english/current-topics/news/ddos-attack-caused-disruption-of-the-availability-of-websites.html (last accessed 30 June 2013); see also 'DigiD brought down by DDoS attack', 25 April 2013. Available at: http://www.telecompaper.com/news/digid-brought-down-by-ddos-attack--939770 (last accessed 30 June 2013).

6 L. Lessig (2001) 'Preface to a conference on trust', *Boston University Law Review*, 81: 330–1.

7 D. S. Anderson (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', *Emory Law Journal*, 54: 1449.

and proposing additional legal instruments, which are to facilitate cross-border electronic commercial transactions, protect users' rights and enhance public safety without jeopardising technological innovation and market development. For example, since 2011 the United Nations Commission on International Trade Law (UNCITRAL) has been working on draft provisions on electronic transferable records.[8] In the EU, the European Commission has been working on a proposal for a regulation on electronic identification and trust services for electronic transactions in the internal market.[9] In China, the Ministry of Commerce of the People's Republic of China also proposed the Regulatory Specifications on the Use of Online Signing Process in Electronic Contracts in 2012 (hereafter 'the Proposed Regulatory Specifications for Electronic Contracts'), together with the Qualification Standard for Electronic Commerce Enterprises.[10]

This chapter will compare different approaches adopted in the international, EU, US and Chinese legislation and their current legislative development, by looking into the definitions, features, benefits and functions of electronic signatures and electronic authentication. It will then analyse a variety of electronic signatures available in the digital market and discuss their level of reliability. Secondly, it will consider the various forms, conditions and requirements of establishing Trusted Third Parties, called Certificate Authorities (CAs), which provide electronic signatures and authentication services at the national and international level. Thirdly, it will examine the duties and liabilities of CAs, especially concerning the liability regime which applies between a CA and a third party who uses the certificate to validate the identity of a certificate holder intending to transact with the third party. Finally, it will propose solutions concerning the international harmonisation of electronic signatures legislation, as well as the possibility of the achievement of a common global consensus on electronic authentication. It is notable that 'the technical standards embedded in electronic contracting technologies will define in important ways the range of communications that prospective contracting parties can exchange',[11] subsequently the technical standards embedded in

8 Draft provisions on electronic transferable records, A/CN.9/WG.IV/WP.122, 4 March 2013.

9 A proposal of the Regulation on 'Electronic Identification and Trusted Services for Electronic Transactions in the Internal Market', European Commission, COM (2012) 238 final.

10 Circular of the Ministry of Commerce of the People's Republic of China, on Soliciting Comments on the Regulations of Online Signing Process of Electronic Contract (Draft), and Circular of the Ministry of Commerce of the People's Republic of China, on Soliciting Comments on Qualification Standard for Electronic Commerce Enterprise (Draft), the Ministry of Commerce, *China Foreign Trade and Economic Cooperation Gazette*, Issue No. 63, October 2012. Available at: http://english.mofcom.gov.cn/article/policyrelease/gazette/201301/20130100015518.shtml (last accessed 30 June 2013).

11 J. Winn (2002–3) 'Emerging issues in electronic contracting, technical standards and law reform', *Uniform Law Review*, pp. 699–711, at p. 701.

electronic signature means and devices will also affect the range of communications chosen that has legal effect.

In general, this chapter argues that although the deployment of digital signatures (advanced) and qualified electronic signatures may increase the reliability of such signatures and in some specific circumstances they may be used as evidence in legal proceedings according to substantive law, there is a need to allow a basic form of electronic signature to have legal effect when it meets the minimum requirements of an international technical standard. It also debates that a harmonised legal regime for the establishment and functioning of certification service providers may help generate trust among trading parties in Certificate Authorities (CAs) and thus facilitate the cross-border recognition of a foreign certificate.

8.1.1 Current legislation: UNCITRAL, 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. The feature and function of a signature was endorsed by one of the leading English cases – *Goodman* v. *J. Eban Ltd*, which outlines a general principle that '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.'[12] It has been recognised that a signature which is 'most closely analogous to a rubber stamp signature' should be given equivalent legal effect.[13] In modern society, using electronic means to sign one's name has been accepted in the same way as a written signature under certain circumstances. Unlike individual manuscript signatures, electronic signatures lack the uniqueness of the written pattern, which necessitate electronic documents to prove trustworthiness and authenticity.[14] Due to the importance that electronic signatures have as the focal point of authenticating electronic records and serving as evidence, regulations on electronic signatures have been adopted at the national, regional and international level since the late 1990s and early 2000s. There are mainly two approaches to e-signatures legislation, namely the minimalist approach and the two-tier approach, though it is also debatable that there is a third

12 *Goodman* v. *J. Eban Ltd* [1954] 1 All ER 763.

13 Rubber stamps affixed to a document can establish valid signatures: *Lazarus Estates, Ltd* v. *Beasley* [1956] 1 QB 702.

14 K. Bharvada (2002) 'Electronic signatures, biometrics and PKI in the UK', *International Review of Law Computers and Technology*, 16 (3): 265–75; see also the EC Directive on Electronic Signatures, Recital 4.

approach known as 'the prescriptive approach'.[15] It is possible that some legislation may amalgamate different approaches.

International legislation

At the international level, currently there are three key legal instruments governing the relevant issues concerning electronic signatures and providing a guide for national and regional legislation:

- UNCITRAL Model Law on Electronic Commerce 1996;
- UNCITRAL Model Law on Electronic Signatures 2001; and
- UN Convention on the Use of Electronic Communications on Electronic Contracting 2005 (hereafter 'the UN Convention').

They are consistent with the form requirements under the United Nations Convention on Contracts for the International Sale of Goods 1980 (CISG). Article 11 of the CISG promotes the principle of freedom from form requirements 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'. The CISG Advisory Council Opinion no. 1 interprets the form requirements as follows: 'A contract may be concluded or evidenced by electronic communications and the term "writing" in CISG also includes any electronic communication retrievable in perceivable form.'[16] It was suggested that if electronic communications would be regarded as writing, the alternative prescribed authentication procedures would be recognised as 'signatures'.[17] The Model Laws and UN Convention concerning electronic communications further clarify and expand the form of signature by electronic means.

Article 7 of the UNCITRAL Model Law on Electronic Commerce employs the minimum approach, specifying the equivalent function of an electronic signature which is to identify the person and approve the data message as long as the methods are reliable and appropriate. This approach provides a technology-neutral and open clause which generates a great degree of flexibility. That is, the features of affixing and logically associating are required as additional conditions to the reliability and appropriateness of an electronic signature to a data message. Article 9 of the UN Convention also reinstates the minimum standards to meet the form requirements as provided in Articles 6, 7 and 8 of the Model Law on Electronic Commerce but does

15 S. Mason (2012) *Electronic Signatures in Law*, 3rd edn (Cambridge: Cambridge University Press), p. 154.

16 CISG Advisory Council Opinion no. 1, Electronic Communications under CISG, 15 August 2003.

17 S. Eiselen (2002) 'E-Commerce and the CISG: formation, formalities and validity', *Vindobona Journal of International Commercial Law and Arbitration*, 6: 305–18, at p. 311.

not intend to allow 'the parties to go as far as relaxing statutory requirements on signature in favour of methods of authentication that provide a lesser degree of reliability than electronic signatures'.[18]

In contrast, the UNCITRAL Model Law on Electronic Signatures adopts the two-tier approach. It defines an 'electronic signature' more specifically as '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'.[19] The first tier (Article 6(1)) is identical to the UNCITRAL Model Law on Electronic Commerce (Article 7) and the second tier (Article 6(3)) further sets specific requirements of an electronic signature to meet the standard of reliability. It requires that an electronic signature: (a) is uniquely linked to the signatory; (b) was created under the control of the signatory; (c) was detectable if altered after signing; and (d) ensures the integrity of the message and that any alteration is detectable. It is notable that the adoption of a two-tier approach does not intend to create restriction on the general recognition and acceptance of an electronic signature as a form of signature. The second tier provides benchmarks to determine the level of reliability when parties are concerned about the identity and integrity of an electronic signature or when national or substantive laws require a signature to meet a certain level of reliability subject to valid authentication.

The recent proposal on the Provisions on Electronic Transferable Records (hereafter 'the Provisions') intends to specifically recognise the legal effect of a particular type of electronic document – electronic transferable records – and enable cross-border recognition of such records for the facilitation of international trade.[20] Article 3 of the Provisions defines 'electronic transferable record' as 'the electronic equivalent of any paper-based transferable document or instrument [that entitles the holder to claim the performance of obligation specified in the electronic transferable record]'. The term 'performance of obligation' refers generally to the delivery of goods or the payment of a sum of money, whereas the term the 'transferable record' refers to documents such as bills of exchange and bills of lading. Article 9 of the Provisions also provides the minimum approach to the recognition of electronic signatures which is in line with that of the UNCITRAL Model Laws and the UN Convention. It is noteworthy that the Provisions would complement the legal effect of 'electronic transport records' in the United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea 2008 and electronic 'bills of exchange' in the United Nations Convention on International Bills of Exchange and International Promissory Notes 1988.

18 Explanatory Note 2007, p. 16.
19 UNCITRAL Model Law on Electronic Signatures (2001), Article 2.
20 Draft provisions on electronic transferable records, A/CN.9/WG.IV/WP.122, 4 March 2013.

EU legislation

The EC Directive on Electronic Signatures[21] also takes the two-tier approach and promotes interoperability of electronic-signature products.[22] It firstly defines the first tier of 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'.[23] It further defines the second tier of an electronic signature as an 'advanced electronic signature', which meets the following requirements:

(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using means that the signatory can maintain under his sole control; and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.[24]

It is noticeable that the advanced electronic signatures which are based on a qualified certificate and which are created by a secure signature creation device enhance the certainty of legal effect as being legally equivalent to handwritten signatures and being admissible as evidence in legal proceedings, although the legal effectiveness and admissibility of advanced electronic signatures cannot be denied solely due to a lack of one of those criteria.[25] The Proposed Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market in 2012 (hereafter 'the EC Proposed Regulation for Electronic Transactions 2012') intends to clarify and expand these provisions by introducing new specific provisions on issues such as the 'legal effects and acceptance of electronic signatures'[26] and the 'requirements for the validation of qualified electronic signatures'.[27] It is notable that the main purpose of these provisions is to ensure a security assurance level with a high level of certainty on the legal effect of electronic signatures. The EC Proposed Regulation for Electronic Transactions 2012 requires the duty of notification and particularly specifies that trust service providers should notify the competent supervisory body for breach of security and loss of data within 24 hours.

21 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures, OJ L 13/12 (19.01.2000).
22 EC Directive on Electronic Signatures, Recital 5.
23 EC Directive on Electronic Signatures, Article 2(1).
24 EC Directive on Electronic Signatures, Article 2(1).
25 EC Directive on Electronic Signatures, Recital (20) and Article 5.
26 COM (2012) 238 final, Article 20.
27 COM (2012) 238 final, Article 25.

US legislation

In the US, the Uniform Electronic Transactions Act (UETA, Sections 5, 7 and 9) takes the minimum approach and simply allows the signature to be accomplished through electronic means. An 'electronic signature' is broadly defined in Section 2(8) as 'an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record'. It is identical to the definition given by the UNCITRAL model laws and the EC Directive, though it explicitly recognises the electronic signature means of 'sound, symbol or process'. Section 7 recognises the legal effect of electronic signatures as the equivalent of handwritten signatures as follows:

(a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.
(b) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.
(c) If a law requires a record to be in writing, an electronic record satisfies the law.
(d) If a law requires a signature, an electronic signature satisfies the law.

Section 9 of the UETA further specifies that if the electronic record or electronic signature resulted from a person's action, it will be attributed to that person, though such attribution shall also be subject to substantive law. It is noticeable that the UETA provides a technology-neutral approach to the creation of a valid electronic signature. Likewise, the US Electronic Signatures in Global and National Commerce Act 2000 (E-Sign Act) also takes the minimum approach (technology-neutral) and provides an identical definition of an 'electronic signature', which is 'an electronic sound, symbol or process, attached to or logically associated with a contract'.[28] However, the E-Sign 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, for instance, clearly indicates that it applies merely to business and commercial transactions in or affecting foreign or interstate commerce.[29] 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 fifty states which would replace all existing state laws currently in effect.[30]

28 US Electronic Signatures in Global and National Commerce Act (E-Sign Act) 2000, Section 106(5); and 15 USC (United States Code) § 7006.

29 E-Sign Act 2000, Section 101(a).

30 S. E. Blythe (2005) 'Digital Signature Law of the United Nations, European Union, United Kingdom and United States: promotion of growth in e-commerce with enhanced security', *Richmond Journal of Law and Technology*, 11 (6): 50.

China legislation

In China, the China Electronic Signatures Law also adopts the two-tier approach, defining an 'electronic signature' as 'data included and attached in a 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'.[31] Article 2 of the China Electronic Signatures Law further defines a data message as 'the information generated, dispatched, received or stored by electronic, optical, magnetic or similar means'. In accordance with the international practice and common standard, the China Electronic Signatures Law adopts the technology-neutral strategy and promotes the principle of party autonomy. It generally acknowledges that 'a reliable electronic signature shall have equal legal force with a handwritten signature or a seal',[32] and 'the parties concerned may also choose to use the electronic signatures which meet the conditions of reliability they have agreed to'.[33]

Article 13 of the China Electronic Signatures Law also provides the determination of a 'reliable electronic signature' (which is equivalent to the 'advanced electronic signature' in the EU Directive on Electronic Signatures and UNCITRAL Model Law on Electronic Signatures) meeting the following conditions:

(1) when the creation data of the electronic signature are used for electronic signature, it exclusively belongs to an electronic signatory;
(2) when the signature is entered, its creation data are controlled only by the electronic signatory;
(3) after the signature is entered, any alteration made to the electronic signature can be detected; and
(4) after the signature is entered, any alteration made to the contents and form of a data message can be detected.

Furthermore, the China Electronic Signatures Law stipulates provisions on 'an electronic verification service' (equivalent to the measures of 'qualified certificate and accredited certification service provider' under the EC Directive on Electronic Signatures). It is fair to say that the China Electronic Signatures Law is a comprehensive legal instrument which meets various international standards, though there are some 'Made in China' rules in this legislation such as the provisions on legal responsibility (in particular Articles 29–31) which stipulate specific figures for a fine and number of years' sentence for compliance failure. It is internationally common that these issues should be dealt with by relevant substantive law instead.

31 China Electronic Signatures Law 2004, Article 2.
32 China Electronic Signatures Law 2004, Article 14.
33 China Electronic Signatures Law 2004, Article 13.

In 2012 the China Proposed Regulatory Specifications on the Use of Online Signing Process in Electronic Contracts (hereafter 'the Proposed Regulatory Specifications for Electronic Contracts') and the Proposed Qualification Standard for Electronic Commerce Enterprises[34] are intended to complement the China Electronic Signatures Law, proposing provisions on 'a signing system of electronic contract', the 'service provider of electronic signature and certificate authentication' and 'third-party storage service providers for electronic contracts'. Article 7.4 of the Proposed Regulatory Specifications for Electronic Contracts affirms that an electronic contract will have an equivalent effect as a paper-based contract if parties give electronic signatures to it. It requires parties to notify the other parties if the data for electronic signature creation is compromised. The duty of notification is consistent with Article 27 of the China Electronic Signatures Law.

It is recognisable that in the UNCITRAL, EU, US and China, there is different wording provided for the definitions of electronic signatures and also various measures adopted for the determination of the effectiveness of electronic signatures. Nonetheless, there is a consensus that electronic signatures can have an equivalent legal effect to handwritten signatures and should be considered as valid means of verifying the identity of the user of a data message or authorising a transaction.

8.1.2 Types of electronic signature

Electronic signatures can take many forms and can be created by many different technologies. Common forms of electronic signatures include but are not limited to the password or personal identification number (PIN), e-mail signatures, smart cards,[35] biometrics,[36] scanned signatures and digital signatures. In daily life, the most common forms of electronic signatures are the PIN, scanned signatures, e-mail signatures and digital signatures.

34 Circular of the Ministry of Commerce of the People's Republic of China, on Soliciting Comments on the Regulations of Online Signing Process of Electronic Contract (Draft), and Circular of the Ministry of Commerce of the People's Republic of China, on Soliciting Comments on Qualification Standard for Electronic Commerce Enterprise (Draft), the Ministry of Commerce, *China Foreign Trade and Economic Cooperation Gazette*, Issue No. 63, October 2012. Available at: http://english.mofcom.gov.cn/article/policyrelease/gazette/201301/20130100015518.shtml (last accessed 30 June 2013).

35 A 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.

36 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.

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 document is known as a Word documented signature. Such a password is also called a '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 signature.

Picture-scanned signatures are also very common. An electronic scanner allows users to scan a piece of paper with a handwritten signature into the computer 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, it is very easy to forge such a file as much less skill and effort is required to scan a paper.

E-mail signatures

An e-mail signature can consist of text or pictures or both. Most e-mail 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's outgoing e-mail messages. In recent years, more and more e-mail signature software has been launched to help users develop a more secure e-mail signature; for example, some signature creation software may help in the creation of 'handwriting' signs/symbols to accent the individuality of the user's signature in e-mail messages.

The legal effect of an e-mail signature is debatable. The UNICTRAL Report on Promoting Confidence in Electronic Commerce in 2007 points out that 'neither typed names on unencrypted e-mail 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.'[37] It is likely that the effectiveness of an e-mail signature may be subject to specific substantive law if the rules of law stipulate specific requirements.[38] It may also be acceptable that 'it would be a matter for legal interpretation whether an electronic form satisfies a particular legal requirement for writing or signature'

37 *Promoting Confidence in Electronic Commerce: legal issues on international use of electronic authentication and signature methods*, United Nations Commission on International Trade Law (UNCITRAL), Vienna, United Nations, 2007 (released in 2009). Available at: http://www.uncitral.org/pdf/english/texts/electcom/08-55698_Ebook.pdf (last accessed 30 June 2013).

38 *DWP Pain Free Med. P.C.* v. *Progressive Northeastern Ins. Co.* 2006 NY Slip Op 26531 [14 Misc 3d 800] December 7, 2006 Hackeling, J. District Court of Suffolk County. It was held that manuscript signatures were required; see also *Wright* v. *Direct Capital Securities, Inc.* 2010 WL 659073 (Cal. App. 4 Dist.)

even if the rule of law uses the wording 'in writing' and 'signed by the party to be charged therewith'.[39] In the Singaporean landmark case of *SM Integrated Transware Pte Ltd* v. *Schenker Singapore (Pte) Ltd*, it was interpreted that names typed in an e-mail correspondence constituted valid signatures.[40]

Digital signatures (advanced electronic signatures)

A digital signature is one of the most important and reliable forms of electronic signatures. From a technical perspective, it is defined as 'an asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature'.[41] Digital signatures 'provide authenticity protection, integrity protection, and non-repudiation'.[42] It is notable that digital signatures and public key infrastructures are important examples of cryptographic technologies which play a major role in ensuring the level of electronic commerce and information system security, though the implementation of such technologies requires appropriate and adequate measures.[43]

Cryptography can be defined as the act of secret writing composed of a series of ciphers and codes used to hide the content of a message. There are two types of cryptography. The first, known as symmetric or secret key cryptography, is an encryption and data authentication method in which both the sender and receiver share the same key.[44] The second is called asymmetric or public key cryptography and utilises two different keys for the encryption and decryption process,[45] which are known as a private key and a public key. 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. That is, these keys are mathematical codes that are different from each other, but are 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.

A simple example of asymmetric or public key cryptography can be given as follows. Assume that A is a sender and B is a receiver. A would like to

39 *SM Integrated Transware Pte Ltd* v. *Schenker Singapore (Pte) Ltd* [2005] SGHC 58.

40 Ibid.

41 Electronic Authentication Guideline, National Institute of Standards and Technology (NIST) US Department of Commerce, Draft NIST Special Publication 800–63–2, February 2013. Available at: http://csrc.nist.gov/publications/drafts/800-63-2/sp800_63_2_draft.pdf (last accessed 30 June 2013), p. 9.

42 Ibid.

43 J. Winn (2001) 'The emperor's new clothes: the shocking truth about digital signatures and Internet commerce', *Idaho Law Review*, 37: 358.

44 Study on the use of cryptographic techniques in Europe, by the European Network and Information Security Agency (ENISA), 2011.

45 K. Bharvada (2002) 'Electronic signatures, biometrics and PKI in the UK', *International Review of Law Computers and Technology*, 16 (3): 265–75, at p. 268.

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. However, this may raise a further concern: how could A know whether the message is really from B or from an impersonator? B may have the same problem regarding to A.

It is notable that there is a need for a trusted third party, such as a Certificate 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 to indicate the intention and authenticate the content.

8.1.3 Benefits and functions

There are two major benefits that can be identified with the use of electronic signatures. The first is the possibility of investigating the reliability of a digital signature by relevant service providers. When an electronic signature is used and the authentication process has been completed, the service providers should be able to let the recipient of the e-mail know whether the e-mail has been tampered with during the process from the sender's computer to the recipient's computer upon request. 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 document has been intercepted and altered en route.

The second benefit of electronic signatures is that they allow for the transmission and receipt of secure e-mails. This is a highly desirable property, especially for lawyers, who will often have to deal with highly sensitive and confidential information. Secure e-mails become possible once one person has another person's public key. The public key can be e-mailed separately to an individual, copied to a disk and sent through the post, or even downloaded from a dedicated website.[46] An example of the digital signature process is as follows. If A wishes to send B a secure e-mail, A will use B's public key to

46 D. Capps (2002) 'Conveyancing in the 21st century: an outline of electronic conveyancing and electronic signatures', *Conveyancer and Property Lawyer*, September/October, pp. 443–55.

encrypt the e-mail and also any documents that are attached. Once encrypted, the only way that the e-mail can be unencrypted is with a public key's corresponding private key. Therefore, if A's public key has encrypted the e-mail, it can only be unencrypted by A's private key. If anyone intercepts the e-mail while in transit, they will be unable to view its contents unless they have a copy of A's private key.[47]

As regards functions, digital signatures can be deemed to be the process of creating, using and verifying a signature which can identify the signer, authenticate the content and serve as evidence for legal proceedings. Firstly, the asymmetric cryptography 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 the 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.[48]

It is noteworthy that qualified electronic signatures (digital signatures) accompanied by an electronic certificate can provide three important functions:

1. authentication – to authenticate the identity of the person who signed the data so it is known who participated in the transaction;
2. integrity – to protect the integrity of the data so it is possible to know that the message read has not been changed, either accidentally or maliciously; and
3. non-repudiation – to enable subsequent proof of who was involved in a transaction, thus preventing anyone from denying that he/she 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.[49]

47 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. Available at: http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf (last accessed 30 June 2013).

48 C. Spyrelli (2002) 'Electronic signatures: a transatlantic bridge? An EU and US legal approach towards electronic authentication', *Journal of Information, Law and Technology*, 2. Available at: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_2/spyrelli/ (last accessed 30 June 2013).

49 S. Baker and M. Yeo (1999) *Survey of International Electronic and Digital Signature Initiatives*, from the Internet Law & Policy Forum Working Group 1999. Available at: http://www.ilpf.org/groups/survey.htm (last accessed 30 June 2013).

When transactions involve several stages at different times, consistency of identity is difficult to prove. For example, how can it be proved who participated in a 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 undertake this transaction? What happens if the decryption key is lost? Who is liable if the decryption key is compromised?[50]

Under these circumstances, verification plays a central role in the process of establishing identity within a Public Key Infrastructure (PKI).[51] 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 pairing has no inbuilt connection with any person. For the purpose of security, persons who are not previously acquainted but 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 Certificate 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.

8.1.4 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.

Likewise, the four evidential requirements in a handwritten signature shall also be fulfilled to qualify as a valid and effective electronic signature. The recognition of the legal effect of an electronic signature has been evidenced both in law and in practice.

In law, it appears that the legal effect of an electronic signature is generally recognised by the most recent international legal instrument – the UN Convention, which affirms the recognition of electronic signatures in previous

50 N. D. Tosto and B. Baracks (1996) *Requirements for a Trusted Global Public Key Initiative*, Information Security Technical Report 27, Vol. 1, No. 1.

51 D. S. Anderson (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', *Emory Law Journal*, 54: 1463.

Model Laws.[52] It was argued that the new development in the UN Convention was that it incorporated and extended the provisions of the Model Laws, introducing an abstract reliability test and method in Article 9(3).[53]

It is generally agreed that electronic signatures should be deemed to be functionally equivalent to handwritten signatures and originals, though certain conditions should be met to create a reliable electronic signature. It is noticeable that the first condition is that the method used should be able to prove the identity of the party and an indication of the party's intention as to the valid form of electronic signature (Article 9(3)(a)). 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'.[54] It is a significant improvement in that it emphasises the identity of the party and the party's intention for the information,[55] while the UNCITRAL Model Law on Electronic Signatures and the UNCITRAL Model Law on Electronic Commerce require 'the integrity of the information which it relates'.[56]

The second condition provided by Article 9(3)(b) is to meet a reliability requirement for the validity of an electronic signature that a 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.

That is, a legal requirement for a signature is met by an electronic means if Article 9(3)(a) is satisfied, and 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'.[57] It is considered that 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

52 UN Convention on the Use of Electronic Communications on International Contracts 2005 (hereafter 'The UN Convention'), Article 9; see also Report of the Working Group on Electronic Commerce on the work of its 42nd session (Vienna, 17–21 November 2003) (A/CN.9/546), at pp. 54–7.

53 S. Mason (2012) *Electronic Signatures in Law*, 3rd edn (Cambridge: Cambridge University Press), p. 102.

54 UNCITRAL Model Law on Electronic Commerce, Article 7(1)(a).

55 The UN Convention 2005, Article 9(3)(a).

56 UNCITRAL Model Law on Electronic Signatures, Article 6(3)(d), and UNCITRAL Model Law on Electronic Commerce, Article 7(1)(a).

57 C. K. Wei and J. C. Suling (2006) 'United Nations Convention on the Use of Electronic Communications in International Contracts – a new global standard', *Singapore Academy of Law Journal*, 18: 116–202, at p. 130.

with Article 9(3)(b)(i). The UN Convention can be deemed to provide an improved solution 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,[58] though the UN Convention has not defined the standards of techniques for being 'as reliable as appropriate' and the specific requirements for further evidence.

National and regional legislation may provide more specific rules as to the determination of an electronic signature being 'as reliable as appropriate' at various levels. For example, as discussed earlier, in the EU the EC Directive on Electronic Signatures which is under review by the Proposed Regulation on Electronic Identification and Trust Service for Electronic Transactions has relevant provisions on the establishment of qualified electronic signatures that advanced electronic signatures are validated by qualified certificates, accredited certification service providers and secure signature creation devices.[59]

In practice, judicial interpretations, which are subject to national substantive laws, may lead to different outcomes under certain circumstances. It is undisputable that the general legal effect of concluding a contract electronically is recognised internationally. For example, in the European Court of Justice (ECJ)/Court of Justice of the European Union (EUCJ) cases, the legal effects of contracting online via an interactive website, and thus signatures given electronically, have been impliedly recognised when the Court determines Internet jurisdiction.[60] There are also national judicial cases recognising the legal effects of concluding a contract electronically in China and the US as discussed earlier in Part II. With regard to the legal effect of electronic signatures, one of the most controversial issues is whether a typed name in the context of an e-mail would form a valid signature.

In the US, in the leading case of *Cloud Corporation* v. *Hasbro. Inc.*, there were several e-mail exchanges between parties focusing on delivery dates and the quantities being described as 'more or less depending on the formula' to be delivered on those dates. It was held that that the sender's name on an e-mail satisfied the signature requirement of the Statute of Frauds without having to rely on the federal Act (the Electronic Signatures in Global and National Commerce Act, 15 USC § 7001).[61]

In contrast, in the leading English case of *Mehta* v. *JPF*,[62] the court came to a different conclusion concerning whether an e-mail bore the signature

58 Ibid.

59 EC Directive on Electronic Signatures 1999, Articles 2 and 5; see also COM (2012)238 final, Articles 20 to 27.

60 Joined Cases C 585/08 and C 144/09, *Peter Pammer* v. *Reederei Karl Schlüter GmbH & Co. KG* (C 585/08) and *Hotel Alpenhof GesmbH* v. *Oliver Heller* (C 144/09), 7 December 2010.

61 *Cloud Corporation* v. *Hasbro. Inc.*, No. 02-1486, 314 F.3d 289 (the United States Court of Appeals for the Seventh Circuit, Dec. 26, 2002); see also *Shattuck* v. *Klotzbach*, No. 011109A, 2001 WL 1839720 (Mass. Super. Dec.11, 2001).

62 *Mehta* v. *JPF* [2006] EWHC 813 (Ch); [2006] 1 WLR 1543; [2006] 2 ALL ER 891, 7 April 2006.

according to the Statute of Frauds. The fact was that Mr Mehta was a director of Bedcare (UK) Ltd. Bedcare failed to pay the supplier, J. Pereira Fernandes (JPF) and ultimately was 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 e-mail to JPF's solicitors for personal guarantee. The e-mail was not signed by Mr Metha but is described in the header as having come from Nelmehta@aol.com. The two key issues at the hearing of the appeal were:

- whether the e-mail constituted a sufficient note or memorandum of the alleged agreement for the purposes of Section 4 of the Statute of Frauds[63]; and
- assuming the e-mail 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 e-mail address on the copy of the e-mail received by JPF's solicitors was a sufficient signature for these purposes.[64]

It is obvious that the focal points here are whether the e-mail was a sufficient memorandum or note, and whether the sender's automatically inserted e-mail address can constitute a signature. Judge Pelling QC considered that the e-mail was indeed a note or memorandum, because the e-mail was in writing and it was not disputed by Mr Mehta that the offer was orally accepted by JPF.[65] As the defendant's name or initials did not appear at the end of the e-mail or in the body of the e-mail, 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.[66] Thus the judge concluded that the presence of the e-mail address at the top of the e-mail did not constitute a signature, following the ruling of *Evans* v. *Hoare*,[67] 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.'[68] The judge regarded the inclusion of an e-mail address in such circumstances as a clear example of the incidental inclusion of a name in the absence of a contrary intention.[69] However, if a party or a party's agent sending an e-mail types his/her or his/her principal's name to the extent required or permitted

63 Statute of Frauds, Section 4.
64 [2006] 1 WLR 1543, p. 1546, para. 10.
65 Ibid., p. 1548, para. 16.
66 [2006] 1 WLR 1543, p. 1550, para. 20.
67 *Evans* v. *Hoare* [1892] 1 QB 593.
68 [1892] 1 QB 593, p. 597.
69 [2006] 1 WLR 1543, p. 1552.

by existing case law in the body of an e-mail, then it would be a sufficient signature for the purposes of Section 4 of the Statute of Frauds.[70]

It is noticeable that, with the advancement of criminals (attackers) utilising information technologies, it is not easy to monitor and detect fraudulent e-mails in an ordinary e-mail system. It is common that while an e-mail may look legitimate, the 'From …' field could have been altered. E-mail recipients cannot merely rely on the sender's e-mail address to validate the true origin of the e-mail. Thus the point debated of whether an e-mail header can constitute a signature should focus on whether the e-mail system is at an appropriate security assurance level to guarantee that the sender is the one that has sent the e-mail, rather than whether the e-mail address itself constitutes a signature. Subsequently, the concern over the legal effect of typed names in e-mails should also focus on the security of the e-mailing system, i.e. whether the e-mail system uses secure portals or layers such as SQL to verify the identity of the e-mail users, rather than the typed form of names contained in the e-mail. If the e-mail systems used are at a higher security assurance level and have not been compromised, nothing can stand in the way of typed names affixed in e-mail correspondences constituting valid signatures as there is sufficient evidence that the e-mail originates from the account owners or authorised users. As a consequence, it is irrelevant to determine the effectiveness based on whether the typed name contained at the bottom of an e-mail as a signature or even an automated signature which the user creates in a fixed box using the signature button in the e-mail system. The level of security provided by a method used is therefore vital to the determination of the legal effect of a valid form of signature in e-mails. Another issue concerning security that needs to be clarified is the interactions between the participants when an agent is involved. For example, imagine a scenario involving a user (as principal), an electronic agent (as agent) and another user (as the third party): the user uses the electronic 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, if something went wrong, the third party could not address the user directly, because the electronic agent has not provided identification of the user. This problem could be solved if the user ratified the actions of the agent, in this way providing his identification to the third party. Another solution, in order to increase the trustworthiness of the use of artificial intelligences, could be the adoption of an agency fiction: if the third party had a reasonable cause to believe the agent acted on behalf of the principal, the principal would be liable.[71] There is a growing need to clarify these issues in legislative reviews and/or with judicial interpretations.

70 [2006] 1 WLR 1543.

71 EU Commission Legal-IST Project, 'Report on Legal Issues of Software Agents', p. 64.

8.2 Electronic authentication

8.2.1 Definition in comparison with electronic signatures

In the traditional environment, authentication and signature do not have the same meaning in different legal systems.[72] In general, authentication is known as a document or piece of evidence connecting with a person, place or thing,[73] while a signature is considered as 'any name or symbol used by a party with the intention of constituting it as his signature'.[74] In most civil law jurisdictions authentication is understood in a narrow scope and a strict way as the authenticity of a document which has been verified and certified by a competent public authority or a notary public.[75]

In the information society, 'authenticate' is firstly defined in the Uniform Computer Information Transactions Act (UCITA) as '(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'.[76] 'Authentication' is understood by the United Nations as satisfying the court when: (1) a document is relevant; (2) a document serves as a piece of evidence; and (3) such evidenced document is connected with a person, place, thing or process.[77] A formal definition of 'authentication' has finally been proposed in the EC Proposal for a Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market in 2012 as:

> an electronic process that allows the validation of the electronic identification of a natural or legal person; or of the origin and integrity of an electronic data.[78]

72 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.

73 *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.

74 *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.

75 *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, 2007 (released in 2009). Available at: http://www.uncitral.org/pdf/english/texts/electcom/08-55698_Ebook.pdf (last accessed 30 June 2013).

76 Uniform Computer Information Transactions Act (UCITA) 1999, Section 102(a)(6).

77 *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, 2007 (released in 2009). Available at: http://www.uncitral.org/pdf/english/texts/electcom/08-55698_Ebook.pdf (last accessed 30 June 2013).

78 COM (2012) 238, final, Brussels, 4 June 2012, Article 3(4).

In 2013, the Electronic Authentication Guideline proposed by the US Department of Commerce defines 'authentication' as 'the process of establishing confidence in the identity of users or information systems',[79] and 'electronic authentication' as 'the process of establishing confidence in user identities electronically presented to an information system'.[80]

It is noteworthy that the concept of 'electronic authentication' is different from 'electronic identification'. 'Electronic identification' refers to 'the process of using person identification data in electronic form unambiguously representing a natural or legal person'.[81] From a technological point of view, electronic authentication can be characterised as the process through which the identity of a computer or network user is verified. From a functional point of view, authentication ensures that an individual is, in fact, who he or she claims to be. Overall, electronic authentication should be deemed not just 'an electronic process' but also 'a means' of providing trustworthy electronic commerce or electronic delivery service, which is used to protect an electronic document from undetected modifications, to provide limited, but reliable, information about a person, and to affirm a signature in an electronic environment, in particular the signer indicating approval of the signed documents. In contrast to electronic authentication, electronic signatures focus particularly on verifying the identity of the owners and deal 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.

'Certificate' is defined as 'an electronic attestation which links electronic signature or seal validation data of a natural or a legal person respectively to the certificate and confirms those data of that person'.[82] Certificates for 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'.[83]

In the EC Proposal Regulation on the Electronic Identification and Trust Services for Electronic Transactions in the Internal Market, a new concept of 'electronic seal' is introduced, which means 'data in electronic form which

79 Electronic Authentication Guideline, National Institute of Standards and Technology (NIST), US Department of Commerce, Draft NIST Special Publication 800-63-2, February 2013. Available at: http://csrc.nist.gov/publications/drafts/800-63-2/sp800_63_2_draft.pdf (last accessed 30 June 2013), p. 6.

80 Electronic Authentication Guideline, February 2013, NIST, US Department of Commerce (800-63-2), p. 9.

81 COM (2012) 238, final, Brussels 4 June 2012, Article 3(1).

82 COM (2012) 238, final, Brussels, 4 June 2012, Article 3(10); see also EC Directive on Electronic Signatures 1999, Article 2(9), which provides a similar definition except for excluding 'seal'.

83 D. I. Bainbridge (2008) *Introduction to Information Technology Law*, 6th edn (Harlow: Pearson Longman), pp. 360–1.

are attached to or logically associated with other electronic data to ensure the origin and the integrity of the associated data.'[84] It is asserted that the functions of electronic seals are to 'serve as evidence that an electronic document was issued by a legal person, ensuring certainty of the document's origin and integrity'[85] and to 'authenticate any digital asset of the legal person'.[86] This definition is not clear in terms of the relationship between electronic seals and electronic authentication. It appears to be logical to understand that an electronic seal is a product (like a stamp) which resulted from the act of electronic authentication of an electronic signature or record.

8.2.2 Trusted third parties: certificate authorities

Definition

A certificate authority (CA) is a trusted third party 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.[87]

A 'CA' has also been known as a 'certification service provider'[88] and 'trust service provider'[89] in the EU and 'electronic verification service provider'[90] in China. It offers a way to confirm that a public key belongs to the claimed owner in an independent way.[91] In the US, the Electronic Authentication Guideline proposed by the US Department of Commerce in 2013 defines a CA as 'a trusted entity that issues and revokes public key certificates' from a technical perspective.[92] That is, a CA does this by issuing or revoking a digital certificate, which associates an individual with a particular public encryption key.[93] The certificate contains the public key and name of the signatory, digitally signed by the CA.[94] That is, to associate a key pair with a prospective signer, a CA issues

84 COM (2012) 238, final, Brussels, 4 June 2012, Article 3(20).
85 COM (2012) 238, final, Brussels, 4 June 2012, Recital (43).
86 COM (2012) 238, final, Brussels, 4 June 2012, Recital (47).
87 Selected Bibliography on Description of Digital Signatures, Appendix 6 on 'The Role of Certification Authorities in Consumer Transactions', prepared by the Internet Law and Policy Forum. Available at: http://www.ilpf.org/groups/ca/app6.htm (last accessed 30 June 2013).
88 EC Directive on Electronic Signatures 1999, Articles 5 to 7.
89 COM (2012) 238, final, Brussels 4 June 2012, Article 3(14). 'Trust service provider' means a natural or a legal person who provides one or more trust services which includes providing 'electronic certificates'.
90 China Electronic Signatures Law 2004, Article 18.
91 M. J. Osty and M. Pulcanio (1999) 'The liability of certification authorities to relying third parties', *John Marshall Journal of Computer and Information Law*, 17 (3): 961.
92 Electronic Authentication Guideline, February 2013, NIST, US Department of Commerce (800-63-2), p. 7.
93 Role of Certification Authorities in Consumer Transactions, prepared by the Internet Law and Policy Forum. Available at: http://www.ilpf.org/groups/ca/draft.htm (last accessed 30 June 2013).
94 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 accessed 30 June 2013), p. 40.

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.

It is notable that a trusted third party such as a CA can play a role as an agent. For example, PayPal enables any individual or business with an e-mail address to securely, easily and quickly send and receive payments online.[95] 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.[96]

Establishment and roles

A CA is established by a public entity or a legal or natural person. The EU, US and China all recognise such form of establishment in their relevant legislation. For example, the EC Directive on Electronic Signatures explicitly provides that:

> Certification services can be offered either by a public entity or a legal or natural person, when it is established in accordance with the national law; whereas Member States should not prohibit certification-service-providers from operating outside voluntary accreditation schemes; it should be ensured that such accreditation schemes do not reduce competition for certification services.[97]

A CA is responsible for the certification process which may interact with the Credential Service Provider (CSP)[98] in the authentication process. The authentication process begins with the Claimant demonstrating possession and control of a token that is bound to the asserted identity to the Verifier

95 See PayPal at: https://www.paypal.com/uk/webapps/mpp/home (last accessed 30 June 2013).

96 PayPal & eBay, *E-Commerce: Safety Guide.* Available at: http://pages.ebay.com/merchantsolutions/PayPal_eBay_eCommerceSafetyGuide.pdf (last accessed 30 June 2013).

97 EC Directive on Electronic Signatures 1999, Recital (12); see also China Electronic Signatures Law 2004, Article 18, and the US Electronic Signatures in Global and National Commerce Act 2000, Section 301(b).

98 Electronic Authentication Guideline, February 2013, NIST, US Department of Commerce (800-63-2), p. 8. A Credential Service Provider (CSP) is 'a trusted entity that issues or registers Subscriber tokens and issues electronic credentials to Subscribers. The CSP may encompass Registration Authorities (RAs) and Verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use.'

through an authentication protocol. Once possession and control have been demonstrated, the Verifier verifies that the credential remains valid, usually by interacting with the CSP.[99] 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 Claimant.

There are several forms of CA available in the electronic market. There are CAs that are licensed (called 'Recognised Certification Authorities (RCAs)'), known as 'qualified trust service providers'[100] or 'accredited certification service providers'[101] in the EU and some other CAs, 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. In the early 2000s some countries imposed a mandatory registration system on all CAs[102] but in recent years most countries such as the EU, US and China have adopted 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' or 'qualified'.[103] The EC Proposed Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market has urged each Member State to establish, maintain and publish trusted lists with information related to the qualified trust service providers.[104] In the US, CAs 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, private companies such as GlobalSign and VeriSign, Inc., supply certifications and related digital services to natural and legal persons. In February 2013 the Certificate Authority Security Council, an advocacy group, was also established in the US to explore and promote best practices that advance the security of websites and online transactions.[105]

It is noteworthy that there are similar core criteria for the establishment of CAs in different countries. In general, a CA needs to comply with a set of requirements to be granted a license, accredited or qualified. The common conditions include financial and technical standards (such as subject qualifications, hardware management, software conditions), competent staff with

99 Electronic Authentication Guideline, February 2013, NIST, US Department of Commerce (800-63-2), p. 23.

100 COM (2012) 238, final, Brussels, 4 June 2012, Article 3(15).

101 EC Directive on Electronic Signatures, Articles 5 and 11.

102 F. Wang (2004) 'Another consideration about legal system of electronic authentication', *Forward Position in Economics*, 2–3: 105–8.

103 COM (2012) 238, final, Brussels, 4 June 2012, Article 19; EC Directive on Electronic Signatures, Annex II; and China Electronic Signatures Law, Article 17.

104 COM (2012) 238, final, Brussels, 4 June 2012, Article 18(1).

105 Certificate Authority Security Council. Available at: https://casecurity.org/ (last accessed 30 June 2013).

expertise, appropriate management procedures and capability of risk management and compensation. The Utah Digital Signature Act was the very first piece of legislation establishing conditions for the establishment of CAs in 1995.[106] The UNCITRAL, EU and China have also adopted relevant provisions on the requirements of the establishment of accredited or qualified trust service providers. They are Article 10 of the UNCITRAL Model Law on Electronic Signatures 2001, Annex II of the EC Directive on Electronic Signatures and Article 17 of the China Electronic Signatures Law. China has also been issuing local measures and notices to enhance best practices of electronic authentication for electronic transactions in various sectors including the health sector and information industry. For example, the Ministry of Industry and Information Technology in the People' s Republic of China issued the Measures for the Administration of Electronic Certification Services 2009[107] in accordance with the China Electronic Signatures Law and other relevant laws to regulate electronic certification services and supervise electronic certification service providers.[108] Article 19 of the EC Proposed Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market proposes detailed requirements for qualified trust service providers including appropriate means of verification, competent staff, sufficient financial resources for risk liability, precise terms and conditions of service, trustworthy systems and products for security and data storage, measures for forgery and theft of data, among others.[109]

In addition, it is also common that national and regional laws may impose a duty of notification on the trust service providers for any breach of security and loss of data integrity. That is, the trust service providers shall notify the competent supervisory body for any breach without undue delay.[110] Moreover, service providers often have a duty to act under certain circumstances with a view to preventing or stopping illegal activities.[111]

Liability

Principles relating to the liability of the trust service providers are specified in Article 6 of the EC Directive on Electronic Signatures. It 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.[112] All certificates,

106 Utah Digital Signature Act 1995, Article 46-3-201.
107 Measures for the Administration of Electronic Certification Services 2009, Order No. 1 of the Ministry of Industry and Information Technology of the People's Republic of China.
108 Measures for the Administration of Electronic Certification Services 2009, Article 1.
109 COM (2012) 238, final, Brussels 4 June 2012, Article 19(1)(2).
110 COM (2012) 238, final, Brussels 4 June 2012, Article 15(2).
111 EC Directive on Electronic Commerce, Recital 40.
112 EC Directive on Electronic Signatures, Article 6.

which include non-qualified certificates, will be subject to national rules regarding liability as they stand now.[113]

In 2012 Article 9 of the EC Proposed Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market proposed the liability provision for the trust service provider as follows:

1. A trust service provider shall be liable for any direct damage caused to any natural or legal person due to failure to comply with the obligations laid down in Article 15(1), unless the trust service provider can prove that he has not acted negligently.
2. A qualified trust service provider shall be liable for any direct damage caused to any natural or legal person due to failure to meet the requirements laid down in this Regulation, in particular in Article 19, unless the qualified trust service provider can prove that he has not acted negligently.[114]

This proposed provision on the liability of the trust service providers is identical to Article 6 of the EC Directive on Electronic Signatures in terms of setting the minimum standard. The wording of this proposed provision makes it clearer in that such liability applies to both 'non-qualified' and 'qualified' trust service providers for only 'direct' damage unless trust service providers can prove that they have not acted negligently. It clarifies three issues:

- both non-qualified and qualified trust service providers should be subject to the standard of liability;
- trust service providers should only be liable for 'direct' damage caused; and
- trust service providers should bear the burden of proof.

It appears that the new EC proposed rule on the 'direct' damage is to strike a balance of the interests and rights among the various parties.

In China, the China Electronic Signatures Law also provides relevant provisions (Articles 27–33) on the liability of the service provider for damage caused to any natural or legal person who relies on the electronic signature issued unless the service provider can prove that he has no fault.[115]

There is something in common in the EU and Chinese legislation concerning the liability of the trust service provider, that is the trust service provider should be liable for negligent acts. The following negligent acts usually amount to the liability of the trust service provider:

1. failure to take proper evidence of the holder's identity;
2. failure to keep proper records, of preventing forged certificates to be produced and of revocations;

113 EC Directive on Electronic Signatures, Recital 22.
114 COM (2012) 238, final, Brussels, 04.06.2012, Article 9.
115 China Electronic Signatures Law 2004, Articles 27–33.

3. failure of staff to include reliable records in certificates; and
4. failure to revoke a certificate after having learned of the error.

One of the controversial issues is how the trust service provider can be exempted from the liability to a third party. A contract of service provided by the trust service provider can be breached by a negligent act of the trust service provider which affects a third party who relies on an incorrect certificate. It is generally recognised that if a third party suffered any loss after having entered into a business relationship with a party on the reliance of an incorrect certificate issued by a CA, then the CA might be held negligent for having failed to thoroughly investigate the accuracy before issuing the certificate, and liable to the party who is relying on that certificate under the law of obligations.[116] That is, parties can sue either for a breach of contract or negligence in tort. In such cases there will be concurrent liability in contract and in tort resulting from a negligent breach of contract. The innocent party could pursue an action in the tort of negligent or he could pursue an action for breach of contract. In the leading English case of *Henderson* v. *Merrett Syndicates Ltd*, it was suggested that:

> When a contractual duty of care overlaps with an essentially similar duty of care imposed by the tort of negligence, a claimant can select whichever cause of action he prefers, or indeed plead both.[117]

That is, a tort and a breach of contract are both civil wrongs. In contract, obligations are generally created and defined by the parties (not the courts). That is, the parties have a choice as to their legal obligations under the contract. In contrast, a tort is committed when an individual fails to conduct his actions in accordance with the standard prescribed by the law. In tort, the duty to act 'reasonably' is imposed by the courts and the courts will compensate an injured party for the loss he/she suffered by the failure of another to act in accordance with this standard.

In contract law, a party who relies on an incorrect certificate (known as 'a third party' or 'the relying party') and is the victim of a financial loss will only be able to sue the CA for a breach of contract if the contract of certification service between the CA and the party expressly provides that a third party may enforce it when a term purports to confer a benefit

116 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, for example, *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).

117 *Henderson* v. *Merrett Syndicates Ltd* [1995] 2 AC 145, HL.

on him.[118] If not, there will be no contractual relationship between the CA and the relying party (a third party). Being outside the contractual sphere, the replying party will have to prove the CA's responsibility on a tortious basis. Often, a CA may be found to be tortiously liable if he was under a duty of care to provide accurate statements, though the scope of that duty of care may depend on the level of inquiry it promised to carry out (i.e. an exemption clause), before issuing the party a certificate.

On the other hand, a relying party should also take reasonable steps to verify the reliability of an electronic signature. For example, Article 11 of the UNCITRAL Model Law on Electronic Signatures 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.[119] Taking into account the difficulty for a third party to prove the CA's negligence due to the complexities of the technical process involved, strict liability should be applicable to the CA and a CA should bear the burden of proof in contractual or tortious liability.[120] Hence, it should be acknowledged that a CA should be strictly liable to any third party for the failure to detect the party's misstatements and have duties to prove a breach of contract or negligence in the actions.

Subsequently it is obvious that it is in CAs' best interests to limit or exempt their liability. In order not to endanger the viability of the CA industry, it is of paramount importance that a CA should not be liable if it acted reasonably. A CA shall 'not be liable for damage resulting from this maximum limit being exceeded'.[121] 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. It is not unusual that many CAs have tried to define and limit their scope of responsibility when issuing certificates in their own documentation. In the US, the documents that define their standards of good practice and liabilities are the Certificate Practice Statement (CPS), which is 'a statement of the practices that a CA employs in issuing certificates',[122] and the Relying Party Agreement (RPA), which 'notifies the relying party of the warranties, disclaimers, classes of certificates, liability

118 S. Hindelang (2002) 'No remedy for disappointed trust – the liability regime for certification authorities towards third parties outwith the EC Directive in England and Germany compared', *Journal of Information Law and Technology*, 1. Available at: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_1/hindelang (last accessed 30 June 2013); see also the UK Contracts (Rights of Third Parties) Act 1999.

119 UNCITRAL Model Law on Electronic Signatures, Article 11.

120 COM (2012) 238, final, Brussels, 04.06.2012, Article 9; see also the EC Directive on Electronic Signatures, Article 6.

121 EC Directive on Electronic Signatures, Article 6(4).

122 M. J. Ostey and M. Pulcanio (1999) 'The liability of certification authorities to relying third parties', *John Marshall Journal of Computer and Information Law*, 17 (3): 961.

limits and limitations of damages applying to an issued certificate'.[123] In 1997 it was suggested that another, 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.[124] In recent years cyber insurance has become more and more popular for individuals and companies to transfer or minimise the risks of data theft and loss. Cyber insurance products are increasingly emerging (i.e. CyberSecurity by Chubb[SM]) and are offered to consumers and businesses that rely heavily on data in e-commerce systems in the market.[125]

International harmonisation: cross-border interoperability and recognition

As discussed, it is notable that there are different approaches in the legislation of the EU, US and China. The fundamental differences in policy orientations and legislative perspectives will hinder, rather than promote, international electronic commerce. The level of trust and confidence businesses and consumers have in the digital environment is dependent upon the successful harmonisation of legislation in e-commerce, e-signatures and e-authentication internationally. The mutual recognition of foreign certificates for electronic signatures is a prerequisite for the successful integration of e-business into the global economy.

The 'functional equivalent' or 'technology-neutral' principle employed in most of the national, regional and international legislation is to enable a degree of flexibility and relevancy in response to the rapid technological changes. In a way such a principle is also helpful to promote cross-border acceptance and recognition of the effectiveness of electronic signatures, authentication and certificates in electronic transactions as evidence in legal proceedings. Some regions have been making efforts towards the harmonisation of cross-border recognition. For example, the EU has been promoting the cross-border recognition of electronic identification, electronic signatures and certificates between Member States in the Action Plan, Digital Agenda and the Proposed Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market.[126] These three legal instruments have further promoted and expanded the principle of the 'interoperability' of

123 Ibid.

124 The Role of Certification Authorities in Consumer Transactions, prepared by the Internet Law and Policy Forum, 14 April 1997. Available at: http://www.ilpf.org/groups/ca/draft.htm (last accessed 30 June 2013).

125 CyberSecurity by Chubb[SM]. Available at: http://www.chubb.com/businesses/csi/chubb822.html (last accessed 30 June 2013).

126 Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market, COM (2008) 798 final of 28.11.2008; Digital Agenda for Europe, COM (2010) 245 of 19.05.2010; and the Proposal for a Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market, COM (2012) 238 final of 04.06.2012.

electronic signature products which was first introduced in the EC Directive on Electronic Signatures (Recitals 5 and 23). For example, the Action Plan has proposed tasks concerning the recognition of foreign electronic signatures and foreign certificates within Member States as follows:[127]

- actions targeted at improving the *interoperability* of qualified electronic signatures and advanced electronic signatures based on qualified certificates, which will clarify the regulatory framework and increase confidence in Certification Service Providers established in another country;
- actions in the medium term to encourage the *interoperability* of advanced electronic signatures, which, in particular, would enable the validity of a signature received from another country to be easily verified;
- actions in the medium term aimed at making e-identification *interoperable.*

In 2010 in the Digital Agenda for Europe, it is recognised that the lack of interoperability is one of the major obstacles to the virtuous circle of the digital economy.[128] The Proposed Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market has proposed a full implementation of 'interoperability' in all disciplines, including the EU-wide cross-border interoperability of electronic signatures, electronic identification, electronic authentication and related trust services (Recital 7 and Article 5); technical interoperability of the notified identification schemes (Recital 15 and Article 8); and interoperability between electronic delivery services (Recital 49 and Article 35). It is noted that 'a lack of interoperability of the electronic signature systems set up at national level' is 'due to the non-uniform application of technical standards' which requires coordination across EU Member States.[129] This further expands the horizon in terms of subject matters concerning the recognition of the third countries' certificates as provided in Article 7(1) of the EC Directive on Electronic Signatures:

> Member States shall ensure that certificates which are issued as qualified certificates to the public by a certification service provider established in a third country are recognised as legally equivalent to certificates issued by a certification service provider established within the Community if: (a) the certification service provider fulfils the requirements laid down in this Directive and has been accredited under a voluntary accreditation scheme established in a Member State; or (b) a certification service provider established within the Community which fulfils the requirements laid down in this Directive guarantees the certificate; or (c) the certificate or the certification service provider is recognised under a bilateral or

127 COM (2008) 798 final.
128 COM (2010) 245.
129 COM (2012) 238 final, p. 5.

> multilateral agreement between the Community and third countries or international organisations.

In addition, the EC Directive on Electronic Signatures (Article 7(2) and (3)) further promotes proposals for the negotiation of bilateral and multilateral agreements with third countries and international organisations in order to facilitate cross-border certification services with third countries and legal recognition of advanced electronic signatures originating in third countries.

In China, Article 26 of the China Electronic Signatures Law also recognises the effect of a foreign certificate for electronic signatures provided that it meets the equivalent criteria, which specifies that:

> Upon examination and approval by the department in charge of the information industry under the State Council on the basis of relevant agreements or the principle of reciprocity, the certificates of electronic signatures issued by overseas electronic verification services outside of the territory of the People's Republic of China shall have equal legal force with the ones issued by the electronic verification services established in accordance with this Law.[130]

In the US, the E-Sign Act (Section 301(a)(1)) is silent on the recognition of foreign certificates but generally promotes the international recognition of electronic signatures:

> The Secretary of Commerce shall promote *the acceptance and use, on an international basis, of electronic signatures* in accordance with the principles specified in paragraph (2) and in a manner consistent with section 101 of this Act. The Secretary of Commerce shall take all actions necessary in a manner consistent with such principles to eliminate or reduce, to the maximum extent possible, the impediments to commerce in electronic signatures, for the purpose of facilitating the development of interstate and *foreign* commerce. (Emphasis added)

In international organisation such as UNCITRAL, Article 12 of the Model Law on Electronic Signatures also promotes the international recognition of foreign certificates and 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.

130 China Electronic Signatures Law 2004, Article 26.

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.

It is worth noting that Article 12 of the UNCITRAL Model Law on Electronic Signatures explicitly recognises foreign certificates and signatures without geographical discrimination, and establishes 'a substantially equivalent level of reliability' as the main test for the recognition 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). It expresses that where parties agree to the use of certain types of electronic signature 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.[131]

In essence, the UNCITRAL Model Law on Electronic Signatures is not designed to bring about equally binding uniform rules throughout the world but 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'.[132]

The Explanatory Note of the UN Convention on the Use of Electronic Communications in International Contract in 2007 further affirms the principle of 'functional equivalence' that:

> The place of origin of an electronic signature, in and of itself, should in no way be a factor determining whether and to what extent foreign certificates or electronic signatures should be recognized as capable of being legally effective in a contracting State.[133]

There is no doubt that international instruments like the UNCITRAL Model Law on Electronic Commerce and the UN Convention on the Use of Electronic

131 UNCITRAL Model Law on Electronic Signatures, Article 12(5).

132 W. J. Craig, 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 accessed 30 June 2013).

133 Explanatory Note 2007, p. 54, para. 158.

Communications in International Contracts are important so as to encourage transnational electronic commercial transactions and build 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.[134] 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 of the legal recognition of foreign certificates and electronic signatures, Working Group IV of the UNCITRAL requested the Secretariat to continue looking into these issues.[135] 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.[136] International obstacles to 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.[137] Business and legal compatibility and the technical interoperability of authentication schemes can be deployed at both the national and the international levels, to facilitate cross-border online interactions and transactions in both the private and public sectors.[138] The UNCITRAL recommends building sophisticated mechanisms for recognising foreign authentication services and working on national rules on the 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' originating from the Model Law on Electronic Signatures (Article 12) should be employed by national laws to enhance the international standard of security and remove the obstacles to the recognition of foreign certificates

134 C. Spyrelli (2002) 'Electronic signatures: a transatlantic bridge? An EU and US legal approach towards electronic authentication', *Journal of Information, Law and Technology*, 2. Available at: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_2/spyrelli/ (last accessed 30 June 2013).

135 A/CN.9/630, p. 1.

136 *Promoting Confidence in Electronic Commerce: legal issues on international use of electronic authentication and signature methods*, United Nations Commission on International Trade Law (UNCITRAL), Vienna, United Nations, 2007 (released in 2009). Available at: http://www.uncitral.org/pdf/english/texts/electcom/08-55698_Ebook.pdf (last accessed 30 June 2013).

137 Promoting Confidence in Electronic Commerce 2007.

138 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 accessed 30 June 2013).

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 service provider. The application of technical interoperability as well as the harmonisation of certificate policies and practice statements will contribute to the promotion of cross-border certification and recognition.

After all, creating trust and building confidence in electronic commerce is of great importance for its development. Special rules for 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 further developed to increase certainty and security in their use with special rules.[139]

139 Promoting Confidence in Electronic Commerce 2007.

9 Data privacy protection: regulations[1]

In the times gone by, spies could enter people's residences, organisations or companies and collect valuable information such as personal sensitive data, trade secrets or transaction records. In the age of the World Wide Web and globalisation, the open architecture of the Internet has generated an environment in which data collection has become much easier,[2] quicker and far reaching than it used to be as a variety of sensitive information can be captured online without a personal presence in the location where the data is situated. It is notable that it is getting harder to keep personal details private as personal data can be stored, processed, distributed or transferred by automated information systems in a split second. For example, on B2C online platforms, an online retailer might have a database of information about its customers' personal details and their history of transactions. On B2B online platforms, 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. Once the security of the online platforms and systems is compromised, mass information may be stolen, misused or sold.

New technologies dramatically change one's lifestyle. It appears that online shopping and social networking have become part of our daily life, while automated transactions via high-frequency trading platforms have grown to be common in financial industries and Google mapping has turned into a daily tool. It is undeniable that Google Street View of towns and cities for Google mapping may contain individuals' sensitive information such as images and vehicle numbers. It was reported that Google collected personal data including full e-mails and passwords from unsuspecting Internet users

1 Part of this chapter draws upon the author's publication: F. Wang, 'Consumer privacy protection in the European Union: legislative reform driven by current technological challenges', in G. Yee (ed.), *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards* (Hershey, PA: IGI Global, 2011), pp. 331–49.

2 R. J. Mann and J. K. Winn, *Electronic Commerce*, 2nd edn (New York: Aspen Publishing, 2005), p. 193.

via wi-fi networks when its Street View cars mapped towns and cities.[3] This raises serious concern over breaches of data privacy.

With the continuing development of technology, automated decision-making on behalf of individuals is also under way. That is, automated agents make decisions for individuals based on the collected data – models of individuals' preferences. Under automated systems, personal data including a long history of individuals' activities, behaviours and habits will be analysed and processed. Individuals may be more vulnerable to attack, because the system contains personal data of increased sensitivity. For instance, the German Federal Constitutional Court in the Judgment of the First Senate of 27 February 2008 (1 BvR 370, 595/07) expressed that 'the use of information technology has taken on a significance for the personality and the development of the individual which could not have been predicted. Modern information technology provides the individual with new possibilities, whilst at the same time entailing new types of endangerment of personality.'[4] The new technologies raise serious concerns on personal data and privacy protection for information an individual provides to a system or captured by a computing program as 'data provided by individual networked systems can be evaluated and the systems made to react in a certain manner' automatically.[5] The endangerments of users' personality are also noted, that is:

> In the context of the data processing process, information technology systems also create by themselves large quantities of further data which can be evaluated as to the user's conduct and characteristics in the same way as data stored by the user. As a consequence, a large amount of data can be accessed in the working memory and on the storage media of such systems relating to the personal circumstances, social contacts and activities of the user. If this data is collected and evaluated by third parties, this can be highly illuminating as to the personality of the user, and may even make it possible to form a profile.[6]

In addition, with the deployment of cloud computing, often data are not stored or processed in one particular data centre within the same country. The standard of data protection can be different between countries and yet businesses and individuals fear that data may not be adequately protected in

3 J. Halliday (2010) 'Google committed "significant breach" over Street View', *Guardian news*, 3 November 2010. Available at: http://www.guardian.co.uk/technology/2010/nov/03/google-information-commissioner-street-view (last accessed 30 June 2013).

4 Case C-595/07, The German Federal Constitutional Court in the Judgment of the First Senate of 27 February 2008,1 BvR 370, para 104. Available at: http://www.bundesverfassungsgericht.de/en/decisions/rs20080227_1bvr037007en.html (last accessed 30 June 2013).

5 1 BvR 370, 595/07, para. 109.

6 1 BvR 370, 595/07, para. 112.

a third country due to different standards in different countries.[7] With the recent invention of Google Glass technology, there is also a growing concern over the 'privacy implications of a device that can be worn by an individual and used to film and record audio of other people'.[8] With the possible future introduction of 'beaming' technology for civilian and commercial uses, a robot can physically represent an individual or legal entity in order to meet with other parties or participate in activities in another place or country, which also raises significant data privacy issues.[9]

In response to the ever fast-growing technology, legislators have been continuously examining and revising the existing rules to be in line with modern technology. It is recognisable that security of data privacy is a vital factor in electronic commerce to boost users' confidence and trust in making electronic commercial transactions. Business organisations that process personal data have been encouraged to take action and adopt privacy-enhancing technological measures. It is considered that data privacy protection measures are beneficial to businesses as the 'payoff' to organisations can be shown in the improvement of customer satisfaction, trust and confidence, the enhancement of reputation and the reduction of legal liabilities,[10] although the regulatory and technological measures on data and privacy protection may contribute to a reduction in transaction speed and an increase in transaction costs. On the other hand, it is debated that the concepts and values of privacy protection have been understood differently, as a consequence privacy may come up the loser when it must be balanced against the cutting-edge imperatives of national security, efficiency and entrepreneurship.[11]

9.1 Definition: data protection v. privacy protection

Data protection and privacy protection have a close relationship which can be understood from a macro perspective: 'Data protection is to protect the rights of data ownership and balance the benefits between the protection of data ownership and the permission of data free-flow, while privacy protection

7 F. Wang (2013) 'Data protection, jurisdiction and cloud computing: the Proposed General Data Protection Regulation', *Intellectual Property Forum*, 90: 98–102, at p. 99.

8 Letter addressed to Google regarding Google Glass, a type of wearable computing in the form of glasses, 18.06.2013, Article 29, Working Party Website. Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm (last accessed 30 June 2013).

9 'Real-world beaming: the risk of avatar and robot crime', *BBC News*, 11 May 2012. Available at: http://www.bbc.co.uk/news/world-europe-17905533 (last accessed 30 June 2013); see also R. Purdy, 'Deliverable D7.2: Scoping Report on the Legal Impacts of BEAMING Technologies', EU FP7 Networked Media and 3D Internet – 248620, 20 July 2011.

10 A. Cavoukian and T. Hamilton (2002) *The Privacy Payoff: How Successful Businesses Build Customer Trust* (Whitby, ON: McGraw-Hill Ryerson) – see generally.

11 J. Cohen (2013) 'What privacy is for', *Harvard Law Review*, 126 (7): 1904–33.

is to protect fundamental human rights.'[12] As stated in Article 8 of the Convention of Human Rights and Fundamental Freedoms (hereafter 'the Human Rights Convention') in 1950, private life should be protected that:

> (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.

The Human Rights Convention (Article 8) shows that the right to privacy is a fundamental human right. Mr Rolv Ryssdal, former 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'.[13]

From a micro perspective, privacy protection is mostly connected with personal data protection, in particular sensitive personal data protection. The European Court of Justice explained that:

> the right to privacy, set out in Article 1(1) of Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, means that the data subject may be certain that his personal data are processed in a correct and lawful manner, that is to say, in particular, that the basic data regarding him are accurate and that they are disclosed to authorised recipients. As is stated in recital 41 in the preamble to the directive, in order to carry out the necessary checks, the data subject must have a right of access to the data relating to him which are being processed.[14]

This explanation highlights the importance of 'correct and lawful data processing' and 'data disclosure to authorised recipients' in relation to the protection of the right to privacy. The amendment of the EC e-Privacy Directive, which is contained in the Directive 2009/136/EC, has justified such importance, which can be found in the provisions of 'Security' and 'Confidentiality'.

12 F. Wang and N. Griffiths (2010) 'Protecting privacy in automated transaction systems: a legal and technological perspective in the EU', *International Review of Law, Computers and Technology*, 24 (2): 153–62, at p. 154.

13 R. Ryssdal, Data Protection and the European Convention on Human Rights, XIII Conf. Data Protection Comm'rs 39, 1991.

14 Case C-553/07, *College van burgemeester en wethouders van Rotterdam* v. *M.E.E. Rijkeboer*, European Court of Justice (Judgment of 7 May 2009).

With regard to the definition of personal data, 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, culture or social identity'.[15]

The further interpretation of 'personal data' in relation to privacy can be found by a leading UK case *Durant* v. *The Financial Services Authority (FSA).*[16] The English Court of Appeal held that personal data only refers to information that affects one's personal or family life, business or professional capacity. The UK Information Commissioner also published a discussion of the implications of the *Durant* case.[17] The Information Commissioner confirmed 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.[18]

The above justification provides helpful guidance and greater clarity regarding the complex meaning of 'personal data' in relation to privacy. However, the EC Directive on Data Protection does not define 'sensitive personal data', although Recitals 34 and 70 of the EC Directive on Data Protection mentions the term 'sensitive' data and Article 8 of the EC Directive on Data Protection refers to 'the processing of sensitive data' without using the wording of 'sensitive'. Article 8(1) of the EC Directive on Data Protection provides that:

> Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

15 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, Article 2(a).

16 *Durant* v. *Financial Services Authority (FSA)* [2003] EWCA Civ. 1746.

17 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.nhsgrampian.org/grampianfoi/files/DurantCase.pdf (last accessed 30 June 2013).

18 *Durant* v. *Financial Services Authority (FSA)* [2003] EWCA Civ. 1746.

So these special categories of data are currently already prohibited as a general rule, with limited exceptions under certain conditions and safeguards. In the UK, the Data Protection Act 1998 clarifies the scope of 'sensitive personal data', which means personal data consisting of information as 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.[19]

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.

On 4 November 2010 the European Commission issued 'a comprehensive approach on personal data protection in the European Union' (hereafter 'the EU Comprehensive Approach 2010') and addressed challengeable legal issues for the communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions.[20] The EU Comprehensive Approach 2010 has identified the importance of understanding the scope of 'sensitive personal data' as it proposes that:

> In the light of technological and other societal developments, there is a need to reconsider the existing provisions on sensitive data, to examine whether other categories of data should be added and to further clarify the conditions for their processing. This concerns, for example, genetic data which is currently not explicitly mentioned as a sensitive category of data.[21]

However, the Comprehensive Approach did not mention about giving a definition of 'sensitive personal data' under the EC Directive on Data Protection.

19 UK Data Protection Act 1998, c. 29.
20 A comprehensive approach on personal data protection in the European Union – Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, European Commission, Brussels, 04.11.2010, COM (2010) 609/3.
21 COM (2010) 609/3, p. 9.

The Proposed EU General Data Protection Regulation 2012 also left out the definition of 'sensitive data protection', though Recital 41 provides that 'personal data which are, by their nature, particularly sensitive and vulnerable in relation to fundamental rights or privacy, deserve specific protection. Such data should not be processed, unless the data subject gives his explicit consent.'[22]

9.2 Challenges of data privacy protection

9.2.1 Unnoticeable technical measures for data collection and processing

When social networking sites, P2P file sharing services, online conferencing and data monitoring tools became available, they dramatically changed the way we live and brought us convenience, efficiency and speed of communications. But it is more and more difficult to detect when and how our personal data is being collected and processed. There are various ways that Internet users' information can be collected and stored without notice and more new ways of data collection and processing have been emerging. Below are some examples.

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 sale promotion; however, it might be used unfairly or unlawfully to sell or share users' clickstream data to a third party.

Computer series number and software product key code registration

Activation of a computer is a mandatory procedure when setting it up, while the registration of software is usually required when installing computer programs. During this process, the service provider might ask you to provide personal information, e.g. address and e-mail, for the record of after-sale service. For example, Microsoft has the 'Windows Product Activation' tool, collecting the users' CPU serial number and CPU model number/type. During activation users may also provide personal information if they want

22 Proposal for a Regulation of the European Parliament and the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), European Commission, Brussels, 25.01.2012, COM (2012) 11 final, 2012/0011 (COD).

to register their product with Microsoft.[23] During other software installments, user registration may also be recommended. It entitles users to receive information about product updates and special offers directly from the service provider, e.g. 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.

Cookies, web bugs, spyware and deep packet inspection

A *cookie* is data or a text file that is sent to users' browsers and stored on users' computer hard drive to track their personal information and visiting or usage patterns. The ostensible purpose of cookies is to facilitate customized services to the user, but the potential for misuse of such data is considerable and well documented.[24] In addition, a cookie can be stolen via the network. In modern browsers, users can be notified when a cookie is sent so they can 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 e-mails and web pages. They can track information on the dispatch of e-mails with the recipient e-mail address. Unlike cookies, they cannot be prohibited by traditional Internet browser settings.[25]

Spyware is another method of information theft. It is software installed surreptitiously on personal computers without the knowledge of the subscriber or user. Such kind of software usually cannot be uninstalled. It is used to gain access to information, store information or trace the activities of the user.[26]

Deep packet inspection is the most sophisticated type of Internet data measurement. It not only analyses the header of an IP packet but also the content (payload). It does so to identify certain types of protocols (such as Skype) that are able to mask themselves and cannot be detected by simpler port-based measurements.[27]

23 Microsoft Windows Product Activation privacy statement. Available at: http://technet.microsoft.com/en-us/library/cc756122.aspx (last accessed 30 June 2013).

24 R. Wacks (2001) 'Privacy reconceived: protecting personal information in a digital world', in E. Lederman and R. Shapira (eds), *Law, Information and Information Technology* (Netherlands: Kluwer Law International), pp. 75–97, at p. 80.

25 R. J. Mann and J. K. Winn (2005) *Electronic Commerce*, 2nd edn (New York: Aspen), p. 194.

26 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 accessed 30 June 2013).

27 Report on Statistical Methodologies on the Internet as a Source of Data Gathering – SMART 2010/0030, 01/09/2012. Available at: http://ec.europa.eu/digital-agenda/en/news/statistical-methodologies-internet-source-data-gathering-smart-20100030 (last accessed 30 June 2013), p.17 (the author of this book – F. Wang – served as the external legal expert in this project).

Online shopping forums

Companies providing online shopping platforms, such as eBay, Amazon and Alibaba, have a large amount of online shoppers' personal information, including name, credit card details, delivery address, e-mail address and product preferences. Such kinds of information are 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 the order, it is unknown whether every company will strictly comply with their policy.

Social networking or online dating sites

Social networking websites, such as Facebook and LinkedIn, 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, may publish and share your sensitive private information, i.e. age, sexual preferences, on their platforms. 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.

Governments, banks or other organisations

There is usually a large profile of personal information stored in the database of governments, banks and other private or public organisations. For example, the domain name registration database WHOIS contains every domain name registrant's details, including domain name address, name, home or company address and telephone numbers, which are published publicly.[28] The BBC also reported that a 'horrifying' number of companies, government departments and other public bodies have breached data protection rules.[29] It will damage social trust and cause social chaos if government agents misuse or trade personal data.

9.2.2 Different legal measures for data collection and processing

Although data privacy, as a fundamental human right, has been protected under basic laws in different countries or conventions at the international

28 .eu Domain Name WHOIS Policy, v.1.0.2. Available at: http://www.eurid.eu/files/whois_en.pdf (last visited on 30 June 2013). Further information can be found at: http://www.eurid.eu/en/content/whois-result (last accessed 30 June 2013).

29 'Firms breaching data protection', *BBC News*, Wednesday, 11 July 2007. Available at: http://news.bbc.co.uk/1/hi/business/6289410.stm (last accessed 30 June 2013).

level since the 1950s, cross-border data protection stemming from open networks has been challenged due to technological and legislative obstacles since the boom in electronic commercial transactions in 2000. Data protection constraints on the Internet are preventing them from fully protecting online users' privacy rights. In order to build the web users' confidence, online trading or service companies have posted self-regulations on web pages. However, it is impossible to know how many users have actually read the data privacy statement in the small print or via a clicked link before using the service or placing the order. It is also debatable whether companies do keep their promises and comply with the self-regulated privacy policies. If not, what are the remedies?

It is notable that breach of data security can amount to criminal charges, tortious liability or contractual liability. The investigatory procedures of breach of data security is subject to national rules of law. The legal measures and remedies for breach of data security are also subject to domestic and regional substantive law. It is inevitable that countries may have different legislative approaches to data privacy protection due to the differentiation in culture, economics, technological constraints and politics. Some countries or regions (such as the EU) have adopted a single data protection and privacy law providing a comprehensive treatment, while others have not adopted a uniform law harmonising the various regulatory protections of data privacy (as in the US and China). This may lead to a collision of international cooperation in enhancing cross-border data protection at a global level.[30]

Subsequently it is difficult to enforce or remedy data privacy protection if the data security is breached in a foreign country. There may be different levels of requirements for data privacy protection in terms of appropriate technical means, informed consent duties, data quality, data processing, rights to be forgotten, rights to access, notification of breach, data retention or statistical research.

The differentiation between national legislation may also affect the effective prevention of cross-border data security breach and amount to the complexity of determining the competent court due to complicated connecting factors such as the establishment of the data controllers and data processors and the location of data centres.This may pose a further threat to data privacy rights protection. In light of these alarming issues, regions or countries such as the EU and US have indicated the necessity of national-level action on the protection of international data transfers and the remedies when breaches occur.

30 P. M. Schwartz (2013) 'The EU-US privacy collision: a turn to institutions and procedures', *Harvard Law Review*, 126 (7): 1966–2009.

9.3 Current legal framework for data privacy protection

9.3.1 International standards: principles

There is no uniform law or convention regulating data privacy protection at the international level, though some international organisations have issued data protection principles and guidelines. For example, the Organisation for Economic Cooperation and Development (OECD) in 1980 and the Asia-Pacific Economic Cooperation (APEC) in 2004 have specified principles for data privacy protection. Some countries have also entered bilateral data privacy protection agreements to enhance cross-border protection between countries such as the US-EU Safe-Harbor Agreement.

The OECD pioneered the international guideline on privacy protection, which sets helpful benchmarks for national legislation. The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data was promulgated in Paris in 1980 (hereafter 'the OECD Guidelines'),[31] which apply to 30 OECD countries, including the UK, US and 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 above eight principles have influenced national and community legislation. For example, the EC Directive on Data Protection in 1995 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 in society, thus its working group started to examine whether the OECD Guidelines were still suitable for the modern information society in the late 1990s and reported its opinion on 'Implementing the

31 Organisation for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Paris, 1980). Available at: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last accessed 30 June 2013).

OECD "Privacy Guidelines" in Electronic Environment: Focus on the Internet' (thereafter 'the OECD Export Report') in 1998.[32] The Export Report reaffirmed that the Privacy Guidelines were applicable with regard to any technology used for collecting and processing data and there was no need to revise the OECD Guidelines, although a dialogue between the private sector and individual users of networks would be useful in order to learn about the needs of business and consider technical solutions.

It is noticeable that the features of online commercial transactions are unique compared with those of offline transactions. Cross-border transfer of data is much easier, faster and wider in the online world. The basic principles on privacy protection of the OECD Guidelines should be still 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 captured in transit via the Internet or sold commercially by electronic means. Trans-border flow of data will naturally raise the volume of cross-border privacy disputes. It challenges the enforcement of transnational cases. It appears that two extra principles – 'transparency' and 'enforceability' – should be considered as additions in the OECD Guidelines. This view is justified by the OECD 'Report on the Cross-border Enforcement of Privacy Laws' in 2006, which states 'greater transparency about how privacy enforcement works would be helpful for business compliance and user trust in global privacy protection'.[33]

Asia-Pacific Economic Cooperation (APEC) has also undertaken the responsibility to harmonise e-privacy international protection standards in order to facilitate economic growth, cooperation, trade and investment in the Asia-Pacific region. In response to the need of an up-to-date international framework on privacy protection, the APEC endorsed the APEC Privacy Framework in 2004, developed by its Electronic Commerce Steering Cooperation. It is based on the core values of the OECD Guidelines. There are 21 APEC member economies including China, the US, Australia and Canada.[34] As mentioned earlier US, Australia and Canada are also 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

32 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, 9 September 1998. Available at: http://www.oecd.org/dataoecd/33/43/2096272.pdf (last accessed 30 June 2013).

33 OECD Report on the Cross-border Enforcement of Privacy Laws. Available at: http://www.oecd.org/dataoecd/17/43/37558845.pdf (last accessed 30 June 2013).

34 Members of the Asia-Pacific Economic Cooperation (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/about-us/about-apec/member-economies.aspx (last accessed 30 June 2013).

developing appropriate privacy protections for personal information, removing barriers to information flows and enabling enforcement agencies to fulfil their mandate to protect information.[35] In other words, its aim is to balance privacy rights and information flow and to enhance enforcement of privacy protection. It reflects the nine principles of the APEC Privacy Framework as follows:

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
9. Collection Limitations.

Compared with the OECD privacy principles, there are two different principles in the APEC Privacy Framework: '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 the protection of 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). The 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'[36] in 2009. This note has taken a number of references from the OECD Guidelines and APEC Privacy Framework, which are intended to provide legal consistency and certainty of privacy protection. It identifies the difficulties in relation to privacy protection in identity management systems,[37] therefore it proposes the issuance of a 'citizen card' by public authorities – an official document for

35 APEC Privacy Framework, 16th APEC Ministerial Meeting, Santiago, Chile, 17–18 November 2004, 2004/AMM/014rev1.

36 Promoting Confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods (hereafter 'Promoting Confidence in Electronic Commerce 2007'), UNCITRAL, Vienna, 2009. Available at: http://www.uncitral.org/pdf/english/publications/sales_publications/PromConfEcom_e.pdf (last accessed 30 June 2013).

37 Promoting Confidence in Electronic Commerce 2007, para. 71.

electronic administrative procedures including commercial transactions to preclude data-sharing issues and protect data privacy.[38] In the author's opinion such identity infrastructure is of a higher level than trustmarks or seal schemes; however, time, cost and privacy concerns may be the most significant barriers to issuing citizen cards at the first stage. At the second stage, technological support might be different in different countries, which might become another obstacle to the promotion of cross-border information flow.

9.3.2 The EU legislative framework

It is noteworthy that 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 it was adopted in 1995.[39] The main purposes of the EC Directive on Data Protection are to protect private life, facilitate the free flow of personal data between Member States[40] and promote the digital economy in Europe. The relationship between the Convention and the Directive can be found in the EC Directive on Data Protection (Recital 10) that:

> 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 of 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.

38 Promoting Confidence in Electronic Commerce, para. 76.

39 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 (thereafter 'EC Directive on Data Protection'), Official Journal L 281, 23/11/1995, pp. 0031–0050.

40 Twenty-eight member states of the EU: Austria, Belgium, Bulgaria, Croatia, 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 accessed 30 June 2013).

(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 protects the fundamental rights and promotes the free movement of data within the EU. It is considered 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.[41] The Proposed General Data Protection Regulation 2012 (Recital 5) affirms that 'technology has transformed both the economy and social life, and requires to further facilitate the free flow of data within the Union and the transfer to third countries and international organisations, while ensuring a high level of protection of personal data.'[42] It also requires that the supervisory authorities should monitor the application and contribute to its consistent application in order to protect natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the internal market.[43]

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

(a) processed fairly and lawfully;
(b) collected for specified, explicit and legitimate purposes;
(c) adequate, relevant and not excessive;
(d) accurate and up-to-date;
(e) keep data subjects permitted for identification for a necessary period only.

Among these five principles, the first principle is fundamental. The EC Directive on Data Protection further explains 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.[44] Articles 16 and 17 specify two additional principles relating the processing of data: confidentiality and security of processing. In addition, the principle of adequacy is adopted to ensure an adequate level of protection for transfer of personal data to third countries.[45] The Proposed General Data Protection Regulation 2012 adds an underlying principle of 'enforcement' that it is time to build a stronger and more coherent data protection framework in the EU, backed by *strong enforcement*

41 C. Kuner (2003) *European Data Privacy Law and Online Business* (New York: Oxford University Press), p. 79.
42 Proposed General Data Protection Regulation 2012, COM (2012) 11 final, Recital 5.
43 Proposed General Data Protection Regulation 2012, COM (2012) 11 final, Recital 96 and Article 46.
44 EC Directive on Data Protection 1995, Article 7(a) and (b).
45 EC Directive on Data Protection 1995, Article 25.

that will allow the digital economy to develop across the internal market.[46] The Proposed General Data Protection Regulation 2012 (Article 45) explicitly provides for 'international co-operation mechanisms for the protection of personal data between the Commission and the supervisory authorities of third countries, in particular those considered offering an adequate level of protection, taking into account the Recommendation by the Organisation for Economic Cooperation and Development (OECD) on cross-border cooperation in the enforcement of laws protecting privacy of 12 June 2007.'[47] It is clear that the Proposed General Data Protection Regulation 2012 endeavours to ensure the enforcement of protection to both personal data and privacy rights.

Although the EC Directive on Data Protection not only protects personal data but also individual privacy rights,[48] there is a need to have a complementary legislation particularising the protection of online privacy and data security in response to new challenges of data privacy protection due to rapid technological developments. Currently there is only one provision in the EC Directive on Data Protection (Article 15) dealing with 'automated processing of data' in relation to the performance of automated information systems. The EC e-Privacy Directive has attempted to enhance this area.[49] The EC e-Privacy Directive (Recital 6) indicates the impact of the Internet on communications services 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 of the EC e-Privacy Directive further specifies the aims to protect the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons in the electronic communications sector. Moreover, the relationship between the EC e-Privacy Directive and the EC Directive on Data Protection is clarified as follows:

> (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

46 Proposed General Data Protection Regulation 2012, COM (2012) 11 final, p. 2 and Recital 6.

47 Proposed General Data Protection Regulation 2012, COM (2012) 11 final, p. 12 and Recitals 100 and 103.

48 EC Directive on Data Protection 1995, Article 1; and see also the EC e-Privacy Directive, Recitals 6 and 12 and Article 1.

49 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31/07/2002, pp. 0037–0047.

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 e-Privacy Directive complements the EC Directive on Data Protection providing privacy protection particularly in the electronic communication sector, some provisions of the EC e-Privacy Directive are narrow or non-specific. For example, Article 4 on Security and Article 6 on Traffic Data need to be amended to regulate the liability of data infringement. On 13 November 2007, the European Commission adopted a Proposal for amending the EC e-Privacy Directive. In response to the proposal, the European Data Protection Supervisor (EDPS) released his second Opinion on EC e-Privacy Directive review and security breach in January 2009.[50] 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.[51] That is, network operators and Internet Service Providers (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'.[52]

In 2009 the revision of the EC e-Privacy Directive under the Directive 2009/136/EC (also known as 'the EU Cookie Directive') provides the relevant provision of 'security of processing' (Article 4(3)–(5)) which responds to the recommendation of a data breach notification system, and inserts an

50 EDPS second Opinion on e-Privacy 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 accessed 30 June 2013).

51 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), OJ C 128/33, 06.06.2009. Available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-01-09_ePricacy_2_EN.pdf (last accessed 30 June 2013).

52 D. Cooper, D. Fink, E. Jones and K. V. Quathem (2006) *Security Breach Notification in Europe on the Horizon*, World Data Protection Report, October. Available at: http://www.cov.com/files/Publication/69e65c7e-4d08-474e-853b-3635e9120777/Presentation/PublicationAttachment/4064434a-7a6e-419e-8996-3c810d88da9c/757.pdf (last accessed 30 June 2013).

article of 'implementation and enforcement' (Article 15(a)). There are three additional sub-sections as additions to the EC e-Privacy Directive (Article 4): 'notification obligations from service providers' (Article 4(3)), 'duty from competent national authorities' (Article 4(4)) and 'adoption of measures resulting from consultation' (Article 4(5)).[53] In addition, Article 5(3) of the EC e-Privacy Directive is replaced by the Directive 2009/136/EC providing the requirement of 'a new consent regime for cookies', 'informed consent' or 'prior consent'. This is also reflected in Recital 66 and Article 6 of the new EC e-Privacy Directive and relevant provision in the Proposed Data Protection Regulation 2012. They clarify the scope, manners and conditions for consent to be valid as a legal ground for lawful processing, and affirm users' rights to be forgotten. It is debatable what constitutes a meaningful consent and whether 'privacy by default' is sufficient.[54] More details concerning 'informed consent' will be discussed in the next chapter.

With regard to the liability of privacy infringement, it is suggested that the substantial issue of the liability of infringement of privacy rights shall be governed by national laws. The EC Directive on Data Protection (Recital 55 and Article 23) provides that 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 e-Privacy Directive also provides that the provisions of judicial remedies, liability and sanctions in the EC Directive on Data Protection shall apply with regard to the national provisions adopted pursuant to this Directive. For example, in the English case of *Applause Store Productions Ltd and Firsht* v. *Grant Raphael*[55] (hereafter the '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 is 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. Judge Richard Parkes QC ruled that the claimant

53 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (text with EEA relevance), OJ L 337, 18.12.2009, pp. 11–36.

54 'Opt-out is not sufficient', European Commission Press Release, 24 June 2010. Available at: http://ec.europa.eu/justice/policies/privacy/news/docs/pr_26_06_10_en.pdf (last accessed 30 June 2013).

55 *Applause Store Productions Ltd and Firsht* v. *Grant Raphael* [2008] EWHC 1781 (QB).

Mathew Firsht was to be awarded £2,000 damages in compensation for his hurt feelings and distress caused by the defendant's misuse of private information, along with other compensation for damages for defamation.

In 2012 the Proposed General Data Protection Regulation further enhanced the provisions of 'remedies, liability and sanctions' (Articles 73–79) which expand relevant provisions in the EC Directive on Data Protection. It is the right of any data subject to lodge a complaint with a supervisory authority and to seek for a judicial remedy against a supervisory authority, a controller or processor.[56] Moreover, Article 77, which builds on Article 23 of the EC Directive on Data Protection, sets out the right to compensation and liability, extends this right to damages caused by processors and clarifies the liability of joint controllers and joint processors.[57] The revised provisions of the 'remedies, liability and sanctions' may ensure a harmonised standard and legal certainty of solutions and compensation for data breach in Member States.

9.3.3 The US approach

While the EU adopts a comprehensive legislation on data privacy protection, the US takes a different approach to such protection which is known as a market-dominated or market-based approach. There is no comprehensive federal legislation towards the protection of data privacy rights, though there are relevant subject-specific statues. For example, the Electronic Communications Privacy Act (ECPA), which was adopted for the telecommunication industry in 1986 before the boom of e-commerce, protects transmissions of electronic data by computer and access to stored electronic communications. Since 1995 the Federal Trade Commission (FTC) has made efforts in recommending online privacy protection.[58] The FTC has surveyed on 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').[59] It was an amalgamation, amendment or improvement of the first two previous reports: *Self-Regulation and Privacy Online: A Federal Trade Commission Report to Congress*[60] in July 1999 and *Privacy Online:*

56 Proposed General Data Protection Regulation 2012, COM (2012) 11 final, Articles 73–76.

57 Proposed General Data Protection Regulation 2012, COM (2012) 11 final, p. 15.

58 FTC Public Speech, 1 November 1995. Available at: http://www.ftc.gov/speeches/varney/varnprvy.shtm (last accessed 30 June 2013).

59 *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 accessed 30 June 2013).

60 *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 accessed 30 June 2013).

A Report to Congress[61] in June 1998. The FTC Fair Information Practices outlines five principles of privacy protection:

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, the OECD Guidelines and the APEC Privacy Framework, plus the unique fifth principle in the FTC report – 'enforcement' – which was not listed as a single separate principle in other national and international privacy policies at that time.[62] Enforcement, as identified by the FTC, is the use of 'a reliable mechanism to impose sanctions for noncompliance with these fair information practices' in any governmental or self-regulatory programme to ensure privacy online.[63] In the self-regulatory industry, the privacy seal programmes are considered to be one of the key enforcement mechanisms to emerge, while in the public sector, the Commission has the authority to seek injunctive and other equitable reliefs or pursue remedies for deceptive information practices that infringe the relevant legislation such as the Children's Online Privacy Protection Act (COPPA).

It is noteworthy that the lack of specific federal data protection legislation in the US may become an obstacle to ensuring a consistent level of data privacy protection and to facilitating cross-border data flow with a third country. According to the EC Directive on Data Protection, personal data will be prohibited from being transferred to non-European Union nations that do not meet the European 'adequacy' level for protection. This might significantly hamper the ability of a third country to engage in many cross-border transactions. 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

61 *Privacy Online: A Report to Congress*, FTC Commission Report, June 1998. Available at: http://www.ftc.gov/reports/privacy3/priv-23a.pdf (last accessed 30 June 2013).

62 F. Wang (2010) *Law of Electronic Commercial Transactions: Contemporary Issues in the EU, US and China* (Oxford: Routledge), p. 115; see also F. Wang (2010) *Protecting Information Privacy on the Internet: Legal Framework in the EU*, Privacy 2010 Proceedings by the AAAI Press (Association for the Advancement of Artificial Intelligence) for AAAI Spring Symposium 2010 – Intelligent Privacy Management Technical Report SS-10-05, 22–24 March, Stanford University, Palo Alto, USA. Available at: http://www.aaai.org/ocs/index.php/SSS/SSS10/paper/view/1093 (last accessed 30 June 2013).

63 FTC Fair Information Practices Report, 2000.

developed a 'safe harbour' framework approved by the EU in 2000.[64] The Safe Harbour Agreement is deemed to be 'an important way for US companies to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by European authorities'.[65] The Safe Harbour Agreement encourages the development of international electronic commercial transactions between the EU and 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 Chapter 10 on Internet privacy. The safe harbour privacy principles are: notice, choice, onward transfer, security, data integrity, access and enforcement.

Most 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, e.g. 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 tracking behaviour and the European Commission has 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 upheld its opinion. On 14 March 2008, EPIC sued the FTC to compel disclosure of documents concerning Jones Day's role in the US DoubleClick merger review.[66]

In 2007 the partnership of the social networking website Facebook.com and 'Beacon' also raised privacy concerns as Facebook users who shop at third-party websites would have their purchases notified to their friends via Facebook. In November 2007, interest group MoveOn.org started a petition campaign and Facebook group against this feature. Facebook was 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 sites.[67]

64 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, 25.08.2000, pp. 7–47.

65 Safe Harbour Overview 2000, US Department of Commerce. Available at: http://export.gov/safeharbor/eu/eg_main_018476.asp (last accessed 30 June 2013).

66 *EPIC* v. *FTC*, Case:1: 08-CV-00448, 14 March 2008.

67 'Facebook executive discusses Beacon brouhaha', *New York Times*, 29 November 2007. Available at: http://bits.blogs.nytimes.com/2007/11/29/facebook-responds-to-beacon-brouhaha/ (last accessed 30 June 2013).

Social networking sites (SNS) have become popular among the younger generation 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 debatable whether the US-EU Safe Harbour Agreement clearly covers the legal requirements of data privacy protection on social networking sites which have been growing fast after the adoption of the 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 the regulation of SNS to ensure compliance with EU law. It has 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.[68] 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 of the EU-US data protection agreement referring to social networking security issues.

The process of coordination and agreement concerning the free flow of data between the EU and the US continues. In January 2012 the Proposed General Data Protection Regulation provided a comprehensive framework for international data transfer and may further expedite cooperation in enhancing an adequate level of protection for data flow between the EU and the US.[69]

In March 2012 the FTC Commission recommended a privacy framework for businesses and policymakers to protect consumer privacy in an era of rapid change, and called on companies to act now to implement best practices to protect consumers' private information.[70] This privacy framework introduces three pillars of best practice, namely:

- Privacy by Design
- Simplified Choice for Businesses and Consumers
- Greater Transparency.

These three pillars are identical to the principles and measures promoted in the EU. For example, privacy by design relates to appropriate technical measures for data collection and processing, while simplified choice and greater transparency relate to informed consent for data collection and processing.

68 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 accessed 30 June 2013).

69 Proposed General Data Protection Regulation 2012, COM (2012) 11 final, Recitals 81–83, Recitals 130–133 and Articles 40–45.

70 Federal Trade Commission (FTC) Report: Protecting Consumer Privacy in an Era of Rapid Change – Recommendations for Businesses and Policymakers, March 2012. Available at: http://ftc.gov/os/2012/03/120326privacyreport.pdf (last accessed 30 June 2013).

9.3.4 The Chinese trend

National legislation

China, similar to the US, currently has no single national data privacy protection law. One of the reasons is possibly the different understanding of privacy in terms of acceptable standards in Chinese traditions and culture. This may be reflected in relevant legislation. For example, Article 66 of the Chinese Civil Procedure Law 1991 provides that 'evidence shall be presented in the court and cross-examined by parties; however, evidence that involves state secrets, trade secrets, or individual privacy shall not be presented in an open court session'.[71] The concept of privacy is often connected with the classification of reputation. For example, Article 140 of the Opinions of the Supreme People's Court on Several Issues concerning the Implementation of the General Principles of the Civil Law of the People's Republic of China (For Trial Implementation) 1988 provides that an act of publicising private and personal information (privacy), which results in certain effects, should be recognised as an infringement of the rights to protect reputation.[72]

It is noteworthy that rules relating to data privacy protection are indirect, simple and non-specific in current Chinese national statutes. In general, privacy rights have been regulated under the Constitution Law 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 China Constitution Law protects the basic rights of personal dignity, providing that '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.'[73] Article 40 of the China Constitution Law provides rights of correspondence such that:

> Freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law. No organization 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.[74]

71 Civil Procedure Law of the People's Republic of China 1991, Article 66.

72 Opinions of the Supreme People's Court on Several Issues concerning the Implementation of the General Principles of the Civil Law of the People's Republic of China (For Trial Implementation) 1988, Article 140.

73 Constitution Law of the People's Republic of China 1982, Standing Committee of the National People's Congress, Article 38.

74 Constitution Law of the People's Republic of China 1982, Article 40.

Article 41(1) of the China Constitution Law protects the general rights of freedom of speech for criticism and suggestions but fabrication or distortion of facts for the purpose of libel or frame-up is prohibited.[75]

Data privacy rights have also been regulated in China Civil Law, though there is no direct clause governing data privacy rights. Article 101 of the General Principles of the Civil Law of the People's Republic of China 1986 specifies 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.[76]

It is noteworthy that selling or illegally providing personal information on citizens may constitute criminal offences and shall, if the circumstances are serious, result in a sentence of imprisonment according to the China Criminal Law (1997, Amendment VII 2009). An Article concerning this is inserted after Article 253 of the Criminal Law 1997 as Article 253(A) in Amendment VII 2009 as follows:

- Where any staff member of a state organ or an entity in such a field as finance, telecommunications, transportation, education or medical treatment, in violation of the state provisions, sells or illegally provides personal information on citizens, which is obtained during the organ's or entity's performance of duties or provision of services, to others shall, if the circumstances are serious, be sentenced to fixed-term imprisonment not more than three years or criminal detention, and/or be fined.
- Whoever illegally obtains the aforesaid information by stealing or any other means shall, if the circumstances are serious, be punished under the preceding paragraph.
- Where any entity commits either of the crimes as described in the preceding two paragraphs, it shall be fined, and the direct liable person in charge and other directly liable persons shall be punished under the applicable paragraph.[77]

On 5 August 2011 the Beijing Second Intermediate People's Court held that 23 defendants, including Hongbo Liu etc., were guilty of making use of their professional positions as employees in the telecommunications industry, illegally obtaining personal information on citizens, selling personal information on citizens and assisting in destroying evidence for the legal proceedings.

75 Constitution Law of the People's Republic of China 1982, Article 41.

76 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, Article 101.

77 Criminal Law of the People's Republic of China, Standing Committee of the National People's Congress of the People's Republic of Law, 1997 and Amendment VII 2009, Article 253(A). Available at: https://www.unodc.org/tldb/pdf/ChineseLegislation/China_Criminial_Law_Amendment_VII_EN.pdf (last accessed 30 June 2013).

For example, Liu, Zhang and Huang registered various tencent QQ accounts and illegally bought personal information in chat rooms. Another defendant Xie used restricted means to obtain location information for over 90 mobile phones and provided them to illegal buyers. The 23 defendants were sentenced from one-year imprisonment to two years and six months' imprisonment with a fine of RMB 30,000 depending on the seriousness of the individual circumstances according to Criminal Law Amendment VII 2009 (Article 253(A)).[78]

It was reported that by the end of December 2012, China had 564 million Internet users with a total of 50.9 million new users and 420 million mobile Internet users, of which rural Internet users accounted for 27.6 per cent of the total in China.[79] With the rapid development of the Chinese information society, there is an urgent need for China to keep up with the legislative developments in data privacy protection in order to: (1) promote a secure environment for international data flow; (2) harmonise different national and local rules so as to provide legal certainties at the national level; and (3) promote confidence in data privacy protection and security in electronic communications.

In December 2012 the Decision on Strengthening Online Information Protection (hereafter 'the Decision 2012'), which has the same legal effect as a law, was adopted by the 94th meeting of the chairman and vice chairpersons of the 11th National People's Congress (NPC) Standing Committee in Beijing.[80] It is the first Decision concerning online information protection at the national level after 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 in 2003. The draft Personal Data Protection Law was published in 2005 and provided rules protecting personal information, data and privacy.[81] The Decision 2012 provides 12 abstract rules on: the prohibition of buying and selling personal information on citizens; the requirement to register real personal identities for telecommunications services; and the requirement for network/Internet service providers to use appropriate technical measures to collect and process data and safeguard personal information. The Decision 2012 provides a

78 Case on Illegal Selling Personal Information in Beijing, Beijing Second Intermediate People's Court, 5 August 2011. Available at: http://bj2zy.chinacourt.org/public/detail.php?id=961 and http://rmfyb.chinacourt.org/paper/page/1/2011-08/06/03/2011080603_pdf.pdf (last accessed 30 June 2013). Tencent QQ is an Internet-based instant messaging platform.

79 The 31st Survey Report on the Internet Development in China, by the China Internet Network Information Center (CNNIC), January 2013. Available at http://www1.cnnic.cn/IDR/ReportDownloads/201302/P020130312536825920279.pdf (last accessed 30 June 2013).

80 China's legislature adopts online info rules to protect privacy, the National People's Congress of the People's Republic of China, 5 January 2013. Available at: http://www.npc.gov.cn/englishnpc/news/Legislation/2013-01/05/content_1750014.htm (last accessed 30 June 2013).

81 'China to legislate for protection of personal information', *People's Daily Online*, 25 January 2005. Available at: http://english.peopledaily.com.cn/200501/25/eng20050125_171801.html (last accessed 30 June 2013).

legislative direction for online information protection, which needs to be transferred into a more detailed national law.

Moreover, in April 2013 a draft amendment to China Consumer Rights Law (1994) was published by the Standing Committee of the National People's Congress (NPC), which includes clarification regarding the protection of personal information and legal measures for commercial fraud as well as provisions concerning online shopping.[82] The Draft of China New Consumer Rights Law (Article 28 as an addition) provides that online shoppers can return goods within seven days after the receipt of goods purchased online and online sellers should refund online shoppers within seven days after goods have been returned. Article 29 as another addition specifies that e-commerce service providers should obtain informed consent from consumers before collecting and processing personal information, use appropriate technical and other measures to safeguard personal information and prevent unsolicited marketing messages by electronic means.[83]

China, as a civil law system country, has legislative methodology that is closer to some continental European countries than the US. The EC Directive on Data Protection 1995, the EC e-Privacy Directive 2002 and the Proposed General Data Protection Regulation 2012 provide models for the future drafting of the China Data Privacy Protection Law. The EU and US bilateral agreements on the free flow of data may also provide an example for the future reciprocal agreements among Hong Kong, Macau, Taiwan and mainland China. To be consistent with the international standard, the future China Data Privacy Protection Law should take into consideration the Guidelines of the OECD and APEC, though the unique traditions, current social legal conditions and culture of the state should be taken into account.

Specific measures, self-regulation and practices

It is known that national and local measures or regulations play a significant role in protecting data security in China. Since 1994 there have been various legislative measures promulgated to address data privacy security concerns. For example, the Regulation of the People's Republic of China for Security Protection of Computer Information Systems was promulgated by Decree No. 147 of the State Council of the People's Republic of China in 1994.[84] In 1997 the Ministry of Public Security of the People's Republic of China

82 'Draft amendment stresses consumer rights', *National People's Congress of the People's Republic of China*, 2 May 2013. Available at: http://www.npc.gov.cn/englishnpc/news/Legislation/2013-05/02/content_1793913.htm (last accessed 30 June 2013).

83 Draft of China New Consumer Rights Law, 28 April 2013. Available at: http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2013-04/28/content_1793762.htm (last accessed 30 June 2013)

84 Regulation of the People's Republic of China for Security Protection of Computer Information Systems, the State Council of the People's Republic of China, Decree No. 147, 1994. Available at: http://www.asianlii.org/cn/legis/cen/laws/rfspocis719/ (last accessed 30 June 2013).

promulgated the Measures for Security Protection Administration of the International Networking of Computer Information Networks.[85]

During 2008 and 2009, several provinces and cities across China also introduced independent local legislative measures. For example, in April 2008 the Regulation of the Guangdong Provision for Security Protection of Computer Information System was also effective. 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.[86] In September 2011 the Standing Committee of the People's Congress in Jiangsu Province issued the Regulation of Information Technology of Jiangsu Province, which includes comprehensive provisions on the collection and use of personal information and liabilities for breach.[87]

Companies running businesses online have also been encouraged to adopt self-regulations and policy on data privacy protection. In November 2012 a national soft law instrument (a self-regulatory guideline) was issued to provide national guidance on the standardisation of personal information protection entitled 'Information Security Technology – Guidelines for Personal Information Protection within Public and Commercial Services Information Systems' (hereafter 'the Guidelines').[88] The Guidelines recommend that the self-regulatory data privacy policy should make sure that users are notified before personal information and in particular sensitive personal data will be collected, processed and transferred. It is also necessary to ensure that data is stored only within a necessary period of time and users have rights to control and access personal information. Technical measures for data security and the liabilities of Internet service providers should be specified. It is considered that the eight principles in the Guidelines should serve as a guide book for companies that adopt self-regulations.

It is of note that self-regulations had been adopted by e-commerce companies in the late 1990s. 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

85 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 accessed 30 June 2013).

86 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://hangzhoufz.gov.cn/fzb/fgk/ywfg200702151.htm (last accessed 30 June 2013).

87 The Regulation of Information Technology of Jiangsu Province, the Standing Committee of the People's Congress in Jiangsu Province, No. 90.

88 Information Security Technology – Guidelines for Personal Information Protection within Public and Commercial Services Information Systems, effective on 1 February 2013. Available at: http://www.npc.gov.cn/npc/xinwen/rdlt/fzjs/2013-03/14/content_1782679.htm (last accessed 30 June 2013).

on privacy protection on the website – 'Privacy Statement' updated on 24 April 2007.[89] 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
11. Exemption of Liability.[90]

This statement is to ensure that the users' personal information will be used correctly and fairly. QQ/Tencent will notify users when collecting their personal information and storing such information in a secured system. In addition, none of the collected information will be shared with a third party unless pre-agreed. It is similar to the seven standard principles of data privacy protection in the EU-US Safe Harbour Agreement[91] except for the principle of Enforcement. There is no enforcement clause in QQ/Tencent's privacy statement and there is also no technology specification for the data security protection system. Moreover, Tencent allows other companies, called third-party ad servers or ad networks, to display advertisements on Tencent web pages 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 who use the QQ/Tencent instant messaging or web service are presumed to have read the privacy statement and agree with the terms and conditions. The problem is whether the users are aware of the privacy statement, and even if they are, whether they will read it carefully before they decide to subscribe to any of the QQ/Tencent products, and even more, whether they will keep paying attention to changes in the privacy statement since 'Tencent will occasionally update this privacy statement' as specified. The users will not necessarily be informed of such kinds of update of the privacy statement as there is no clause on the duty of notification of amendment to the privacy policy.

89 About Tencent (QQ). Available at: http://www.tencent.com/en-us/at/abouttencent.shtml (last accessed 30 June 2013)

90 QQ/Tencent Privacy Statement. Available at: http://www.tencent.com/en-us/le/privacy.shtml (last accessed 30 June 2013).

91 EU-US Safe Harbour Privacy Principles: Notice, Choice, Onward Transfer, Security, Data Integrity, Access and Enforcement.

The second distinguishing example of the development of China's online privacy policy 'Alibaba.com' founded in 1999 – one of the world's largest online B2B marketplaces providing a trading platform for global small and medium manufacturers.[92] The privacy policy of Alibaba.com (the global trade platform) was updated and published on 1 January 2009, while the privacy statement of Alibaba.com.cn (the Chinese domestic trade platform) remained unchanged from 1999. Alibaba.com.cn clarifies that when users agree to the Service Agreement, they agree to the privacy statement as it is part of the Service Agreement.[93] The statement lists the provisions of (1) the protection of children; (2) usage of username and password; (3) usage of users' registration information, i.e. name, address, nationality, phone number and e-mail address; (4) usage of cookies; (5) conditions of transferring information to a third party; and (6) 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 the 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 or exchange users' personal information unless a third party affiliates or forms a partnership with Alibaba to support the operation of the site and services. Alibaba will comply with relevant security measures ensuring 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 Alibaba.com.cn specialises in Chinese domestic trade. It is an interesting finding that within the same organisation, different branches promoting sales and production in different jurisdictions have separate or different privacy policies. The privacy policy of Alibaba.com is newer than that of Alibaba.com.cn. They are both similar; however, compared with Alibaba.com.cn, Alibaba.com has more advanced clauses regarding information collected (including not only registration information and statistical information in Alibaba.com.cn but also publishing information and payment information); the transfer of information collected to a third party; and amendments to the privacy policy. Alibaba.com specifies that information collected will not be disclosed to such third parties unless the users respond to the marketing, promotion or advertising message. Information collected may be transferred, stored, used and processed outside the home jurisdiction. In case of a merger with or transfer of business to another business entity, the company will transfer information collected to the entity. Any changes of policy will be posted on the website. If users do not agree to the new changes

92 About Alibaba. Available at: http://news.alibaba.com/specials/aboutalibaba/index.html (last accessed 30 June 2013).

93 Policy Statement of Alibaba.com.cn. Available at: http://info.1688.com/biznews/pages/alihome/js_ys.html (last accessed 30 June 2013).

in the Privacy Policy, they should contact Alibaba.com in writing.[94] Again, as with Alibaba.com.cn and QQ/Tencent, a duty of notification of changes in policy is not required.

The Alibaba privacy policies raise a 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? It is considered that the 2012 Self-regulatory Guidelines for Personal Information Protection within Public and Commercial Services Information Systems,[95] which correspond with international best practices, may provide guidance to businesses and raise Internet users' awareness of how businesses and consumers ensure a fair level of data privacy protection.

In summary, there seems to be a certain level of consensus concerning data privacy principles at a global level such as in the OECD, APEC, EU-US Safe Harbour Agreement, US FTC guidelines, EC Directives and recent Chinese legislative measures. The common principles of 'accountability', 'notification', 'choice', 'security', 'data integrity', 'accessibility', 'admissibility' and 'enforceability' are clearly recognisable. This can be deemed the first step in promoting a harmonised international standard of data privacy protection in the global information society, though the implementation of these principles at national and regional levels requires continuous efforts in sharing best practices, adopting appropriate technical and legislative measures and enabling cross-border enforcement of remedies, liabilities and sanctions.

94 Privacy Policy of Alibaba.com. Available at: http://www.alibaba.com/trade/servlet/page/help/rules_and_policies/privacy_policy (last accessed 30 June 2013).

95 Information Security Technology – Guidelines for Personal Information Protection within Public and Commercial Services Information Systems, effective on 1 February 2013. Available at: http://www.npc.gov.cn/npc/xinwen/rdlt/fzjs/2013-03/14/content_1782679.htm (last accessed 30 June 2013).

10 Data privacy protection: practices and implementation[1]

In 2013 it was reported that hundreds of different apps are added to the apps stores daily and these apps are able to collect large quantities of data from smart devices in order to process services.[2] It is likely that many apps may access data such as contacts, pictures, videos and other personal documents stored on smart devices.[3] It is inevitable that the implementation of the core principles of data privacy protection at the national, regional and international levels may be further challenged by the pace of new technological developments. Consequently continuous efforts are needed to ensure data privacy protection in the changing technology environment by sharing best practices, adopting appropriate technical and legislative measures and enabling cross-border enforcement of remedies, liabilities and sanctions. It could be argued that the current EU legislative framework on data privacy protection is coherent and comprehensive, though practices in certain areas (i.e. implementation and international coordination) may need to be further assessed and strengthened accordingly. Nevertheless the EU legislative framework may be considered a pilot study of best practices for international organisations and other countries. The focal points of 'informed consent', 'data breach notification' and 'effective enforcement mechanisms' will be analysed so as to form a sample model for legislative references.

10.1 Informed consent[4]

Consent is one of the central legal grounds for collecting and processing data information as well as monitoring users' behaviours for statistical research on

1 Part of this chapter draws upon the author's publication F. Wang (2011) 'Personal data breach notification system in the European Union: interpretation of "without undue delay"', *European Business Law Review*, 22 (6): 741–57.

2 WP202 – Opinion 02/2013 on apps on smart devices by the Article 29 Working Party, European Commission, 00461/13/EN, 27 February 2013. Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf (last accessed 30 June 2013).

3 WP202, p. 14.

4 Part of this section draws upon the author's work on the project: Statistical Methodologies on the Internet as a Source of Data Gathering – SMART 2010/0030, 01/09/2012 (F. Wang served as the external legal expert in this project).

market developments before users can explicitly give consent or install add-ons on their operating systems. In 2009 the amended EC e-Privacy Directive[5] particularises and complements the EC Directive on Data Protection regulating the special category concerning 'informed consent' for data privacy protection in electronic communications. In 2012 the Proposed General Data Protection Regulation further enriched the scope and required manner of 'informed consent'.[6]

The requirement of 'informed consent' corresponds with the principle of 'confidentiality' which has been previously regulated in Article 5 of the EC e-Privacy Directive and Article 16 of the EC Directive on Data Protection. The revised Article 5(3) of the EC e-Privacy Directive is intended to give further explanation of Article 16 of the EC Directive on Data Protection that very briefly states:

> Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.[7]

The replacement of Article 5(3) of the EC e-Privacy Directive has introduced the principle of 'the consent given by the subscriber or user concerned' for the storing of information or the gaining of access to information already stored in terminal equipment (e.g. mobile phones or laptops). It provides as follows:

> 3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned *has given his or her consent*, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. (Emphasis added)

5 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, and Regulation (EC) No. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, Official Journal of the European Union, L 337/11, 18 December 2009, pp. 0011–0036.

6 Proposed General Data Protection Regulation 2012, COM (2012) 11 final, Recitals 25, 31–34, 40–41, 53, 55, 58, 86,123, 129 and 131, and Articles 4(8), 6(1), 7–9, 17, 18(2), 20(2), 44 and 83(2).

7 EC Directive on Data Protection 1995, Article 16.

This takes a two-tier approach to the process of 'informed consent': the first tier is that the subscriber or user must be informed and provided with clear and comprehensive information; and the second tier is that the subscriber or user must give consent before information can be accessed, collected, processed and stored.

The enhancement of 'informed consent' (also known as 'prior consent') is also reflected in Recital 66 and Article 6 of the new EC e-Privacy Directive that service providers must inform users before obtaining their consent about the type of data that is collected and the duration and purposes of processing and storage of such data, and service providers shall allow users to give and withdraw their consent freely as users have 'the right to be forgotten'. Under the new EC e-Privacy Directive, the use of cookies on websites also requires users' prior consent. It was also suggested that the principle of consent may need to be further considered for situations where the combination of data from different sources is allowed such as key-coded data, location data and 'data mining' technologies, or cases where the confidentiality and integrity in information-technology systems must be ensured.[8]

It is undisputable that 'explicit' consent is required for the processing of sensitive personal data,[9] though it is debatable what constitutes a meaningful consent and whether 'privacy by default' is sufficient. The conditions of constituting valid consent for processing personal data under the current EU legal legislation are 'freely given', 'specific', 'informed' and 'unambiguous'.[10]

Article 29 Working Party on Data Protection addressed the situation that 'currently three out of the four most widely used browsers have a default setting to accept all cookies. Not changing a default setting cannot be considered as a meaningful consent.'[11] Opinion 2/2010 on Online Behavioural Advertising (WP171) affirms that 'prior-opt in consent mechanisms are better suited to deliver informed consent' and asks 'advertising network providers to create prior opt-in mechanisms which requires an affirmative action by the data subjects indicating their willingness to receive cookies or similar devices and the subsequent monitoring of their surfing behaviour for the purposes of serving tailored advertising'.[12] Furthermore, Opinion 15/2011 on the Definition

8 A comprehensive approach on personal data protection in the European Union – Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, European Commission, Brussels, 04.11.2010 COM (2010) 609/3, p. 5; see, for instance, the judgment by the German Federal Constitutional Court in the Judgment of the First Senate of 27 February 2008,1 BvR 370/07.

9 EC Directive on Data Protection 1995, Article 8(2).

10 EC Directive on Data Protection 1995, Articles 2(h) and 7(a).

11 Opt-out is not sufficient: European Commission Press Release, 24 June 2010. Available at: http://ec.europa.eu/justice/policies/privacy/news/docs/pr_26_06_10_en.pdf (last accessed 30 June 2013).

12 WP171 – Opinion 2/2010 on Online Behavioural Advertising by the Article 29 Data Protection Working Party, 00909/10/EN, 22 June 2010. Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf (last accessed 30 June 2013).

of Consent (WP187)[13] provides Member States with more detailed guidelines on what constitutes a valid consent. It confirms that there are two steps for users to give consent: firstly, users must show indication of wishes; and secondly, users must signify the agreement. Thus silence or lack of action from users could not be considered valid consent. It also reinforces the requirement that the data controller should make sure that 'individuals concerned must be given, in a clear and understandable manner, accurate and full information of all relevant issues';[14] demonstrate that 'consent was obtained based on specific and understandable information';[15] and create and retain 'evidence showing that the consent was indeed given'.[16] The data controller should adopt relevant measures and procedures to make sure that consent is given and verifiable, i.e. put in place 'recordable consent mechanism'.[17] As a result, 'not clicking a box' or 'a pre-ticked box' in an online context should not be used as a valid form of obtaining users' consent, in particular regarding sensitive personal data, while 'online tick boxes' or 'dialogue boxes' could be feasible provided that information on the purposes of data collection and ways to signify consent are specific, easily noticeable, seen and understood by users. It is noteworthy that this opinion seems to be stricter than the earlier opinion of the European Data Protection Supervisor that consent could be inferred from an action of the individual (e.g. the action consisting of using a website is deemed as consenting to logging users' data for marketing purposes) or from silence or inaction (e.g. not un-clicking a ticked box is deemed to be consent).[18]

It is considered that 'informed consent' shall be collected in a user-friendly manner and users should not be disrupted unnecessarily during the usage of services. The ECJ case *Deutsche Telekom AG* confirmed that for some purposes of data processing, consent only needs to be obtained once.[19] Further processing of data for historical, statistical or scientific purposes shall not be considered incompatible with the principles of data privacy protection provided that appropriate safeguards are in place.[20]

The obligation of 'informed consent' is applicable to any type of electronic communications and services such as social networking sites, apps on smart

13 WP187 – Opinion 15/2011 on the Definition of Consent by the Article 29 Data Protection Working Party, 01197/11/EN, 13 July 2011. Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf (last accessed 30 June 2013).

14 WP187, p. 12.

15 WP187, p. 20.

16 WP187, p. 21.

17 WP187, p. 26.

18 Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – 'A comprehensive approach on personal data protection in the European Union' (2011/C 181/01), OJ, C181, 22 June 2011, pp. 10–11.

19 Judgment of the Court Case C-543/09, *Deutsche Telekom AG Bundesrepublik Deutschland* v. *GoYellow GmbH*, Telix AG, 5 May 2011.

20 EC Directive on Data Protection 1995, Article 6(b).

devices and cloud computing services. For example, in the US, Google was ordered to obtain express affirmative consent from the Google user prior to any new or additional sharing by respondent of the Google user's identified information with any third party.[21] In the EU in one of the leading ECJ cases *Lindqvist*, the court held that disclosing personal information on an Internet page without prior consent constitutes the processing of personal data wholly or partly by automatic means within the meaning of Article 3(1) of the EC Directive on Data Protection.[22] This means that users of social networks, apps providers and cloud service providers acting as controllers processing and/or disclosing personal data of other individuals fall within the scope of data privacy protection under the EU legislative framework. It is suggested that app developers and app stores for smart devices should design and implement a security-friendly environment in line with the principles of 'purpose limitation and data minimisation' and require users' consent prior to the installation of apps.[23] In the cloud environment, the cloud processor may subcontract its activities for sub-processing, but it is only permitted after clearly informing the controller of any intended changes with the prior written consent of the controller and with a written agreement imposing the same obligations on the sub-processor as are imposed on the processor. [24] This is to ensure an adequate level of security for data collection and processing.

The concept of 'informed consent' is further interpreted by the Proposed General Data Protection Regulation 2012 in the EU. For example, it clarifies the wording of 'unambiguous' consent in Article 4(8) that in the definition of consent, the criterion 'explicit' is added to avoid confusing parallelism with 'unambiguous' consent and in order to have one single and consistent definition of consent, ensuring the awareness of the data subject that, and to what, he or she gives consent.[25] It states:

> The data subject's consent' means any *freely* given *specific*, *informed* and *explicit* indication of his or her wishes by which the data subject, either by a statement or by a *clear affirmative action*, *signifies* agreement to personal data relating to them being processed.(Emphasis added)

21 See *Google, Inc.*, FTC Docket No. C-4336 (Oct. 13, 2011) (complaint and consent order). Available at: http://www.ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf (last accessed 30 June 2013), pp. 3–4.

22 ECJ, Case C-101/01, *Bodil Lindqvist*, 6.11.2003, and the *Satamedia* Case C-73/07, *Tietosuojavaltuutettu* v. *Satakunnan Markkinapörssi Oy, Satamedia Oy*, 16.12.2008, para. 44.

23 WP202, pp. 14 and 19.

24 WP196 – Opinion 05/2012 on Cloud Computing by the Article 29 Data Protection Working Party, 01037/12/EN, 1 July 2012. Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf (last accessed 30 June 2013), pp. 9–10.

25 Proposed General Data Protection Regulation 2012, COM (2012) 11 final, Article 4.

The conditions of the data subject's consent are further provided in Article 7, which should be paired with the controller's obligation of informing and providing information provided in Articles 11(2) and 14. Article 11(2) of the Proposed General Data Protection Regulation requires that:

> The controller shall provide any information and any communication relating to the processing of personal data to the data subject *in an intelligible form*, using *clear and plain* language, adapted to the data subject, in particular for any information addressed specifically to a child.

Together these provisions in the Proposed General Data Protection Regulation establish a two-tier approach identical to that provided in the new EC e-Privacy Directive discussed earlier but places more specific and detailed conditions on both tiers:

- The first tier is that the subscriber or user must be informed and provided with clear and comprehensive information in an intelligible form, using clear and plain language.
- The second tier is that the subscriber or user must give consent that is freely given with specific, informed and explicit indication of wishes by making a statement, taking a clear affirmative action or signifying agreement before any information can be accessed, collected, processed and stored.

It is clear that a comprehensive framework for the implementation of 'informed consent' is provided by the Proposed General Data Protection Regulation, which endorses, enhances and extends this requirement in all areas of practices concerning privacy data protection in electronic communications.

10.2 Data breach notification

It is noteworthy that personal data breach may lead to serious consequences. It was reported that the UK branch of Zurich Insurance Plc (Zurich UK) had lost 46,000 customers' personal details due to data security failings, including identity details and in some cases bank account and credit card information, details about insured assets and security arrangements. The UK Financial Services Authority (FSA) has fined Zurich Insurance Plc £2,275,000 for failing to have adequate systems and controls in place to prevent the loss of customers' confidential information as the loss could have led to serious financial detriment for customers and even exposed them to the risk of burglary.[26] In response to the alarming risk of data loss in information systems, appropriate technical measures must be adopted by service providers. In case of data

26 'News: FSA fines Zurich Insurance £2,275,000 following the loss of 46,000 policy holders' personal details', 24 August 2010, FSA/PN/134/2010. Available at: http://www.fsa.gov.uk/pages/Library/Communication/PR/2010/134.shtml (last accessed 30 June 2013).

breach, there should be suitable measures promptly employed to minimise the loss. The mechanism of data breach notification is therefore established to provide rescue measures and facilitate the coordination between service providers and competent supervisory bodies. Most countries have acknowledged the importance of such mechanisms, though the level of deployment varies among countries. In the US data breach notification systems have also been employed by the Federal Trade Commission for data privacy enforcement. In China the concept of data breach notification has also been adopted in recent legislative measures and guidelines.

The abstract concept of the data breach notification mechanism was first mentioned in Article 15(2) of the EC Directive on Electronic Commerce:

> Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.[27]

The mechanism of data breach notification has been gradually maturing during the process of the revision of the EC e-Privacy Directive, the review of the EC Directive on Data Protection and the adoption of the Proposed General Data Protection Regulation. The process of reinforcing the data breach notification mechanism started when the concept of 'personal data breach' was added in the revised EC e-Privacy Directive. It means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community.[28] The EU Comprehensive Approach 2010 has proposed an examination of the modalities of a personal data breach notification system in the general legal framework, including details such as the addressees of such notifications and the criteria for triggering the obligation to notify.[29]

10.2.1 Security of processing: data breach notification duty

There are seven general principles set out in the old EU Directives on data privacy protection: security, confidentiality, data quality, onward transfer,

27 EC Directive on Electronic Commerce 2000, Article 15(2).

28 EC e-Privacy Directive amended by the Directive 2009/136/EC, Article 2(h).

29 A comprehensive approach on personal data protection in the European Union – Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, European Commission, Brussels, 04.11.2010 COM (2010) 609/3, p. 7.

choice, notice and access. There are also five sub-principles with regard to data quality set out in Article 6 of the EC Directive on Data Protection, while there are six sub-principles concerning the transfer of personal data to a third country set out in Article 25 of the EC Directive on Data Protection.

As discussed earlier, the principle of enforceability has also been added under the new Article 15(a) of the EC e-Privacy Directive. However, one of the most common principles specified by the OECD in 1980 and APEC in 2004 still has not been highlighted in the EU data privacy legislation: accountability. Accountability mechanisms fall into two categories: one is structure and the other is transparency.[30] The issue of transparency in data privacy protection has been raised by the EU Comprehensive Approach 2010. The Approach has proposed the introduction of 'a general principle of transparent processing of personal data in the legal framework' accordingly.[31] The Proposed General Data Protection Regulation also reinforces the principle of transparency in Recital 46 that:

> The principle of transparency requires that any information addressed to the public or to the data subject should be easily accessible and easy to understand, and that clear and plain language is used.[32]

Among the general principles, security and confidentiality are particularly enhanced by the new EC e-Privacy Directive. 'Security' is one of the most essential principles for personal data and privacy protection. The original Article 4 of the e-Privacy Directive provides the provision of 'security' that:

1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.
2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the

30 F. Wang (2009) *Online Dispute Resolution: Technology, Management and Legal Practice from an International Perspective* (Oxford: Chandos Publishing), p. 73.

31 A comprehensive approach on personal data protection in the European Union – Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, European Commission, Brussels, 04.11.2010 COM (2010) 609/3, p. 6.

32 Proposed General Data Protection Regulation 2012, COM (2012) 11 final, Recital 46; see also Articles 11–13.

service provider, of any possible remedies, including an indication of the likely costs involved.

As shown above, the provision of 'security' under the EC e-Privacy Directive introduces 'taking appropriate technical and organisational measures' and 'informing duty' to safeguard security in a descriptively conceptual way. The Directive 2009/136/EC makes efforts to increase the legal certainty of security by providing more detailed explanations and procedures. The Directive 2009/136/EC changes the title/provision heading of Article 4 of the e-Privacy Directive from 'Security' to 'Security of Processing' and inserts one sub-section in Article 4(1) and three additional sections as Article 4(3)–(5) targeting mandatory personal data breach notification measures etc. of the previous provision. The EC e-Privacy Directive and the Directive 2009/136/EC particularise and complement the Data Protection Directive by translating the principle of security set out in the EC Directive on Data Protection into specific rules.

The change of title of Article 4 demonstrates the importance of the 'processing' stage for the protection of personal data and privacy. Article 4(1a) of the Directive 2009/136/EC further emphasises the processing part of ensuring security which makes sure that 'personal data can be accessed only by authorised personnel for legally authorised purposes'. It requires the protection of 'personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure' and ensures 'the implementation of a security policy with respect to the processing of personal data'. It also suggests that 'relevant national authorities shall be able to audit the measures taken by providers of publicly available electronic communication services and to issue recommendations about best practices concerning the level of security which those measures should achieve'. The wording of the insertion (Article 4(1a) of the Directive 2009/136/EC) brings consistency to the data protection principles outlined in Articles 6, 7 and 17 of the EC Directive on Data Protection, that is personal data must be processed fairly and lawfully.

Moreover, the European Data Protection Supervisor (EDPS) welcomes the adoption of a security breach notification system as it will encourage business organisations to improve data security and enhance the accountability of the personal data.[33] That is, network operators and Internet Service Providers (ISPs) should notify the National Regulatory Authorities (NRAs) and also their customers of security breach. This recommendation has been adopted in the amendment of the EC e-Privacy Directive under the Directive 2009/136/EC and set up under the provision of 'security of processing'.

33 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), OJ C 128/33, 06.06.2009.

There are three additional sub-sections: 'notification obligations from service providers' (Article 4(3)), 'duty from competent national authorities' (Article 4(4)) and 'adoption of measures resulting from consultation' (Article 4(5)).

Article 4(3) added to the Directive 2009/136/EC provides the key requirements of 'notification of personal data breach' from the service provider that:

> [I]n the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority. When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay. Notification of a personal data breach to a subscriber or individual concerned shall not be required if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it. Without prejudice to the provider's obligation to notify subscribers and individuals concerned, if the provider has not already notified the subscriber or individual of the personal data breach, the competent national authority, having considered the likely adverse effects of the breach, may require it to do so.

The above sub-section continues with the specification of requirements on to whom the notification shall be made. They are twofold: one is to the competent national authority; the other is to the subscriber or individual. For the purposes of this Article, as for much of this Directive, the competent national authority refers to the Information Commissioner's Office (ICO).[34]

The service provider should notify the competent national authority of the personal data breach in the first instance. There is no requirement of notification of a personal data breach to a subscriber or individual concerned if the provider had demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach.[35]

With regard to the notification content to the subscriber or individual, the service provider is required to describe the nature of the personal data breach and the contact points where more information can be obtained, and shall

34 Implementing the revised EU electronic communications framework: overall approaches and consultation on specific issues, Department for Business, Innovation and Skills (BIS), September 2010. Available at: http://www.bis.gov.uk/Consultations/revised-eu-electronic-communications-framework (last accessed 30 June 2013).

35 EC e-Privacy Directive, Article 4(3).

recommend measures to mitigate the possible adverse effects of that breach. With regard to the notification content to the competent national authority, the service provider is required to provide additional information describing the consequences of, and the measures proposed or taken by the provider to address, the personal data breach.

The further insertion of 'duty from competent national authorities' (Article 4(4) of the EC e-Privacy Directive) particularises the specific requirements of competent national authorises to give support and guidance and enhance the implementation certainty. According to these two inserted sections, the competent national authorities are encouraged to adopt guidelines and issue instructions to the notification of personal data breaches for service providers as well as impose appropriate sanctions in the event of a failure to comply with notification obligations. Another insertion of 'the Commission's adoption of measures resulting from consultation' (Article 4(5) of the EC e-Privacy Directive) specify the role of the Commission as a guardian to adopt appropriate technical implementing measures following consultation with agents, working parties and supervisors.

The EU Comprehensive Approach 2010 has raised discussion on possible solutions to ensure consistency in implementation of technological protection measures. For instance, it suggests introducing modalities and using one or more EU standard forms ('privacy information notices') by data controllers.[36]

10.2.2 Future legislative reform of the data breach notification system

There is no doubt that the new EC e-Privacy Directive has been modernised to be compatible with the current technology in order to protect the users' data privacy rights and enhance public safety. However, technologies have continued to grow fast leaving legislators with no choice but to re-examine constantly the existing rules.

For example, drivers who wish to park their cars on the streets of London but have no coins or cash at hand can phone and pay the car parking service by quoting a specific street parking location number, vehicle registration number, parking period, name and credit card number according to the parking instruction post on the side of the streets. Some months later, if he/she wants to use this service again, he/she only needs to call, quoting their name, the specific street parking location number and the last four digits of his/her credit card. The transaction can be done automatically using the stored information/data. With the further development of automated information

36 A comprehensive approach on personal data protection in the European Union – Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, European Commission, Brussels, 04.11.2010 COM (2010) 609/3, p. 6.

systems, it is not hard to imagine that, in a few years' time, when we park our cars, our credit cards will be automatically charged for the parking fee without any human interaction as the automated system will immediately identify where we are and what we are doing.

Such automated decision-making systems can equally apply to other industries such as travel agencies. The automated travel agent can design and offer a most favourable travel package to an individual based on the information that the individual gives and other data sources that the agent collects such as passenger records, vehicle traffic records, health conditions and annual incomes, etc. This is also known as 'service-oriented computing'. Apart from the functional development of computing technology, the growth in the capacity of computing facilities is also astonishing. It is suggested that the capacity of a computer is doubled every 18 months which means that after a period of 15 years, the processing and storage capabilities of our computers have increased by a factor of 1,000.[37] It implies that personal data will be more largely captured, widely used, heavily stored and broadly analysed in the future automated computing service systems. Personal data protection, therefore, will be greatly challenged due to the large-scale development in computing functions, speed of processing and storage capabilities. There is an increasing need of further considerations on matters such as the time limit of notification obligations and remedies on data privacy infringements.

10.2.3 Timeframe of notification

The new EC e-Privacy Directive requires that in the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority. The provider of publicly available electronic communications services refers to public and private electronic communications sectors and horizontally to all business organisations that process certain types of information.

As discussed earlier, the update of Article 4 of the EC e-Privacy Directive introduces the concepts and requirements of 'notification of data breach' and 'duty from competent national authorities'. It well reflects on the principles set out in Articles 12(c) and 28 of the EC Directive on Data Protection. However, it does not specify a timeframe for the notification of data breach except for the requirement of 'without undue delay'. Moreover, it does not introduce modalities of the notification of data breach except for the recommendation of guidelines and instructions that may be adopted by competent national authorities. The EU Comprehensive Approach 2010 has identified the necessity of introducing modalities for providing information and drawing up one or more EU standard forms ('privacy information notices') to be

37 R. Wacks (2010) *Privacy: A Very Short Introduction* (New York: Oxford University Press), p. 127.

used by data controllers, but it is silent on the necessity of interpreting 'without undue delay' for the notification of data breach.

In the author's opinion, the interpretation of 'without undue delay' is vital as the timing affects the certainty of data privacy protection. The determination of the appropriate time limit on notification and remedial action shall take into account the speed, scope and capabilities of spreading personal data under the current and future development of technologies, in particular automated information systems. In addition, consideration of the time-limit issue for notification and remedial action can be learned from the interpretation of the time-limit requirement on the exercise of the right to access in Article 12(a) of the EC Directive on Data Protection regarding information storage and disclosure in the case of *College van burgemeester en wethouders van Rotterdam* v. *M.E.E. Rijkeboer Netherlands* (judgment of 7 May 2009).[38] The judgment provides that:

> Article 12(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 requires Member States to ensure a right of access to information on the recipients or categories of recipient of personal data and on the content of the data disclosed not only in respect of the present but also in respect of the past. It is for Member States to *fix a time-limit* for storage of that information and to provide for access to that information which constitutes *a fair balance* between, on the one hand, the interest of the data subject in protecting his privacy, in particular by way of his rights to object and to bring legal proceedings and, on the other, the burden which the obligation to store that information represents for the controller.
>
> Rules limiting the storage of information on the recipients or categories of recipient of personal data and on the content of the data disclosed to a period of *one year* and correspondingly limiting access to that information, while basic data is stored for a much longer period, do not constitute a fair balance of the interest and obligation at issue, unless it can be shown that longer storage of that information would constitute an excessive burden on the controller. It is, however, for national courts to make the determinations necessary.[39] (Emphasis added)

Accordingly, it shall be up to Member States to fix a time limit for notification of the personal data breach and remedial action. Where the length of time within which a personal data breach is to be informed to the competent national authority or remedial action is to be taken is very long, the adverse

38 Case C-553/07, *College van burgemeester en wethouders van Rotterdam* v. *M.E.E. Rijkeboer, European Court of Justice* (Judgment of 7 May 2009).

39 Ibid, para 71.

effects of the breach of the personal data or privacy of a subscriber or individual may be higher as the implementation of appropriate technological protection measures may be delayed. The issue of a fixed time limit for notification and remedial action shall be further assessed when the Commission examines the modalities for the introduction in the general legal framework of a general personal data breach notification, including the addressees of such notifications and the criteria for triggering the obligation to notify according to the EU Comprehensive Approach 2010. The obligation of a time limit for notification of data breach shall also be contained in EU standard forms of privacy information notices in the future.

To avoid undue delay in the notification of data breach, the adoption of regulatory and technological measures of enhancing data controllers' responsibility shall be encouraged. According to the EU Comprehensive Approach 2010, the Commission considers measures to enhance a data controller's responsibility including making the appointment of an independent Data Protection Officer mandatory and harmonising the rules related to their tasks and competences, while reflecting on the appropriate threshold to avoid undue administrative burdens, particularly on small and micro-enterprises, inserting an obligation for data controllers to carry out a data protection impact assessment in specific cases and further promoting the use of Privacy-Enhancing Technologies (PETs) and the possibilities for the concrete implementation of the concept of 'Privacy by Design'.[40]

With regard to the issue of the necessity of reporting data breach to a subscriber or individual in addition to the competent national authority, in the author's opinion, specific conditions shall be considered:

- Whether it is necessary to report data breach to a subscriber or individual shall depend on the breach recovery status. For example, it shall not be required if the provider has demonstrated the satisfaction of remedial action to the security breach to the competent authority according to Article 4(3) of the revised EC e-Privacy Directive.
- Whether it is necessary to report data breach to a subscriber or individual shall depend on the harmful effects of notification, for example panic and social threat.
- Whether it is necessary to report data breach to a subscriber or individual shall depend on the size of the breach effects, such as the threshold for the direct cost of personal data breach and the potential incremental cost resulting from notification, the number of affected individuals and the scale of harm.

40 A comprehensive approach on personal data protection in the European Union – Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, European Commission, Brussels, 04.11.2010 COM (2010) 609/3, p. 12.

If notification of a personal data breach to a subscriber or individual is necessary, the time limit of such notification shall be concerned in particular regarding the time period between notification to the competent national authority and notification to a subscriber or individual, because the provider is required to notify the personal data breach to the competent national authority in the first instance according to Article 4(3) of the revised EC e-Privacy Directive. Therefore there shall be two different time periods for notification of data breach without undue delay: the first time period should be considered that the provider shall notify the competent national authority of a personal data breach as soon as the provider has noticed the breach and no later than 24 hours of having learned of such breach; and the second time period should be considered that the provider shall notify a personal data breach to a subscriber or individual when necessary within 24 hours after the notification of the personal data breach to the competent national authority. In other words, the competent national authority shall assess the satisfaction of the provider's implementing appropriate technological protection measures and inform the decision of notification to a subscriber or individual within 24 hours of the receipt of the case.[41]

The time limit of notification of a personal data breach shall be considered, proposed and included in the guidelines and instructions issued by competent national authorities. As discussed earlier Article 4 of the new EC E-Privacy Directive recommends competent national authorities adopt guidelines and issue instructions on notification for the personal data breach. The EU Comprehensive Approach 2010 proposes that data protection authorities should strengthen their cooperation and better coordinate their activities, [42] because the consistent measures rely on the cooperation between competent national data protection authorities especially when data breach issues have a cross-border dimension. For example, when multinational enterprises are based in several Member States and are carrying out their activities in each of these countries, they might need the guidance from different national authorities and coordinated supervision from the European Data Protection Supervisor (EDPS). An unambiguous procedure for cooperation between data protection authorities will help in dealing with the notification of data breach from multinational business organisations/service providers more efficiently and better implement the 'undue delay notification' duty.

In response to various debates over 'without undue delay' and standardised forms of notification, Article 31 of the Proposed General Data

41 F. Wang (2011) 'Personal data breach notification system in the European Union: interpretation of "without undue delay"', *European Business Law Review*, 22 (6): 741–57, at p. 753.

42 A comprehensive approach on personal data protection in the European Union – Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, European Commission, Brussels, 04.11.2010 COM (2010) 609/3, p. 12.

Protection Regulation also provides a specific and comprehensive provision on 'notification of a personal data breach to the supervisory authority', stating that:

> 1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.
> …
> 6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein …

On 24 June 2013 the European Commission adopted a Regulation on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC on privacy and electronic communications to be effective on 25 August 2013.[43] It affirms the timeframe of data breach notification in that telecommunications operators and Internet service providers shall notify the competent national authority of a data breach within 24 hours of its detection where feasible.[44] This should been deemed as an initial notification. A second notification with more detail should follow within three days after the initial notification.[45] However, the timeframe regarding notification of personal data breaches to the subscriber or individual where there is likely to be adverse effect remains unclassified as 'without undue delay'.[46] The deployment of 'without undue delay' for the notification of personal data breaches to the subscriber or individual can be understood to be 'as soon as possible when appropriate'. This may minimise the risk of unnecessary panic and negative impact on a subscriber or individual and reduce the possibility of compromising evidential materials or attracting further attacks.

43 Commission Regulation (EU) No. 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications (hereafter 'Regulation on the Notification of Personal Data Breaches 2013'), OJ L 173/2, 26 June 2013. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:EN:PDF (last accessed 30 June 2013).

44 Regulation on the Notification of Personal Data Breaches 2013, Article 2(2).

45 Regulation on the Notification of Personal Data Breaches 2013, Article 2(3).

46 Regulation on the Notification of Personal Data Breaches 2013, Article 3(3).

10.3 Effective enforcement mechanisms

The modernisation of existing legislation is of practical necessity, while enforcement is of fundamental importance, because any legislative and technological measures to protect consumers' privacy can only be effective if they are properly implemented and enforced. The implementation of the '24 hours' time bar and the 'without undue delay' requirement for notification of the personal data breach is fundamentally important to enhance the quality control of data protection, reduce the risk of potential personal harm and financial loss as well as increase consumers' confidence and trust in using automated information systems. According to Article 4(4) of the revised EC e-Privacy Directive, the service providers should be liable for breach of the 'without undue delay' obligation. As discussed, the Proposed General Data Protection Regulation 2012 further enhances the provisions of 'remedies, liability and sanctions' (Articles 73–79) which expand relevant provisions in the EC Directive on Data Protection and affirm the right of any data subject to lodge a complaint with a supervisory authority and seek a judicial remedy against a supervisory authority, a controller or processor.

That is, the mechanisms of enforcement are threefold: the first is by national enforcement authorities; the second is by court litigation; and the third is by out-of-court resolutions or self-regulatory enforcement initiatives.

10.3.1 National enforcement authorities

With regard to national enforcement authorities, in the UK the enforcement authority is the information commissioner, whereas in the US the enforcement authority is the federal trade commissioner. As to the exercise of the power of national enforcement authorities, national enforcement authorities can impose sanctions or fines for privacy breaches. For example, in the EU the competent national authority shall impose appropriate sanctions on service providers in breach of the notification obligation according to Article 4(4) of the revised EC e-Privacy Directive. Article 15(a) of the revised EC e-Privacy Directive further particularises the implementation and enforcement of the provisions of the Directive ensuring Member States lay down the rules on penalties including criminal sanctions and enhance the power of competent national authorities in terms of order, investigation and cross-border cooperation. It was reported that 'the lack of a legal obligation for service providers to report data breaches in some member states may aggravate the weakness of the enforcement system',[47] thus Member States shall amend national laws including the introduction of the data breach notification system in order to

47 'Data Protection in the European Union: the Role of National Data Protection Authorities', European Union Agency for Fundamental Rights (FRA) (Luxembourg: Publications Office of the European Union, 2010), p. 43.

comply with the revised EC e-Privacy Directive. National laws shall ensure that competent national authorities have access to effective sanctions on the breach of the 'without undue delay' notification duty of the service provider. Competent national authorities may also be allowed to impose a civil monetary penalty for breach of the 'without undue delay' notification depending to the nature and effects of individual cases according to national laws.

10.3.2 Court litigation or judicial remedies

As regards court litigation, the EU Comprehensive Approach 2010 considers that it is essential to have effective provisions on remedies and sanctions that the Commission will consider:

> the possibility of extending the power to bring an action before the national courts to data protection authorities and to civil society associations, as well as to other associations representing data subjects' interests; and assess the need for strengthening the existing provisions on sanctions, for example by explicitly including criminal sanctions in case of serious data protection violations, in order to make them more effective.[48]

However, it is time-consuming and complicated to enforce privacy protection in the courts and it is even more complex when the dispute concerns the transfer of data between EU Member States or from the EU to a third country outside the EU Member States due to the challenges of ascertaining jurisdiction and applicable law. Currently there is only one main article concerning conflict-of-law rules in the EC Directive on Data Protection (Article 4).

10.3.3 Out-of-court resolutions or self-regulatory enforcement initiatives

The adoption of self-regulatory enforcement initiatives may avoid the complication of determining jurisdiction and choice of law. The initiatives have been strongly encouraged by the FTC Fair Information Practices Report in 2000, the OECD Privacy Online: Policy and Practice Guidance in 2003 and the EU Comprehensive Approach in 2010. Self-enforcement is encouraged as both OECD Privacy Online: Policy and Practice Guidance[49] in 2003 and

48 A comprehensive approach on personal data protection in the European Union – Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, European Commission, Brussels, 04.11.2010 COM (2010) 609/3, p. 9.

49 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 accessed 30 June 2013).

FTC Fair Information Practices Report in 2000 found that fostering the adoption of self-regulatory enforcement mechanisms or initiatives, such as trustmark/seal programmes, will be beneficial to promote 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 website. 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. The well-known seal/trustmarks programmes are TRUSTe, BBBOnline and VeriSign. Some companies' websites have been licensed by the online privacy seal programme, for example eBay and Microsoft licensed by TRUSTe, Alibaba.com accredited by VeriSign, etc. However, currently privacy seal programmes are not widely supported by international and national legislation and only a relatively small percentage of sites have introduced an online privacy seal programme.

Both TRUSTe and BBBOnline have their enforcement procedures: users filing a complaint and seal programme providers responding to a complaint by imposing sanctions on accredited websites. Such kind of sanctions may include:

- requiring the licensee to correct or modify personally identifiable information or change user preferences;
- requiring the licensee to change its privacy statement or privacy practices; and/or
- 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.[50]

However, seal programme providers cannot require a licensee to pay monetary damages or take further steps to exempt his/her liability in violation of law. The TRUSTe Transparency Report will be published annually providing an in-depth summary and analysis of the consumer privacy disputes TRUSTe processed, while TRUSTe should maintain the secrecy and confidentiality of collected information.[51] TRUSTe and BBBOnline are the sole judges of the dispute.

50 TRUSTe Dispute Resolution. Available at: http://www.truste.com/products-and-services/dispute-resolution-services/; BBBOnline Complaints. Available at: https://www.bbb.org/consumer-complaints/file-a-complaint/get-started (last accessed 30 June 2013).

51 TRUSTe Transparency Report, available at: http://www.truste.com/about-TRUSTe/transparency-report, and TRUSTe Terms of Service, available at: http://www.truste.com/terms-of-service (last accessed 30 June 2013).

Mann and Winn recognised that the kind of complaint forum provided by TRUSTe and BBBOnline is an alternative dispute resolution (ADR) mechanism.[52] In the author's view, the TRUSTe Watchdog Dispute Resolution Forum and BBBOnline Compliant Forum are not arbitration, mediation or negotiation as their standards are much lower than those of ADR procedures. This raises some concerns over 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 and much more trustworthy or reliable and professional to adopt an efficient ODR procedure as cases of privacy breaches are usually not very simple. They require expert investigation.

Seal programmes' ODR service can be provided by any of two means. The first method would be that seal programme 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 a partnership with independent ODR service providers and publish the appointment agreement that seal-accredited privacy policy disputes would be resolved by their ODR partner. It is worthy of note that, as mentioned earlier, eBay is accredited by the TRUSTe seal programme, while it is compulsory for eBay users' disputes to be resolved by SquareTrade (an ODR service provider) first 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 users' confidence in providing personal information to proceed with commercial transactions.

A 'mark' or 'seal' should be deemed 'a readily recognizable emblem, voluntarily displayed on a Web site, which signifies that a site has met recognized industry privacy requirements'.[53] A trustmark or privacy seal programme can be beneficial for promoting effective enforcement on data privacy protection compliance including the assessment of the compliance with the 'without undue delay' data breach notification duty. Currently, the best known providers for online privacy seals are the American companies such as TRUSTe, BBBOnline and VeriSign. These seal programmes have been designed to meet the conditions of the international regulations and US-EU Safe Harbour Agreement. They have procedures in common: users

52 R. J. Mann and J. K. Winn (2005) *Electronic Commerce*, 2nd edn (New York: Aspen Publishing), p. 227.

53 'Online Privacy Seal Program', US Chamber of Commerce. Available at: http://www.uschamber.com/issues/technology/online-privacy-seal-programs (last accessed 30 June 2013).

can file a complaint to a seal programme provider and the seal programme provider will respond to a complaint by imposing sanctions on accredited websites. However, as discussed earlier, those privacy seal programmes cannot require a licensee to pay monetary damages or take further steps to be exempt from penalty in law. In the EU, the European Commission has proposed to explore the possible creation of EU certification schemes (e.g. 'privacy seals'). The idea is to provide standardisation for 'privacy-compliant' processes, technologies, products and services to be used by both individuals and data controllers.[54] The Commission will examine how privacy seals fit in with the legal obligation and international technical standards, and propose measures to ensure the trustworthiness of such privacy seals. In the author's opinion, a regulation or guideline on privacy seals might be necessary to introduce the consistent conduct of privacy seal providers that opt for certified technologies, products or services in Member States. Such regulation shall provide a stronger institutional arrangement for the effective enforcement of data protection rules including the obligations and liabilities of service providers and the role of competent national data protection authorities.

In the EU, due to the fact that the current provisions on self-regulation (code of conduct) in Article 27 of the EC Directive on Data Protection have rarely been used so far and are not considered satisfactory by private stakeholders, the European Commission continues to encourage data controllers to employ self-regulatory initiatives so as to establish a better enforcement system. It is known that a trustmark or privacy seal programme is one of the most common recommended self-regulatory initiatives on data privacy protection. The Proposed General Data Protection Regulation 2012 further concerns codes of conduct building on Article 27 of the EC Directive on Data Protection,[55] which also emphasises the inclusion of 'out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data'.[56] It adds an additional requirement that draft codes of conduct shall be submitted to the national supervisory authority to decide on the general validity of codes of conduct.[57] The establishment of data certification mechanisms and data protection seals and marks has also been encouraged in the Proposed General Data Protection Regulation, which seeks the proper application of this EU Regulation taking into account the specific features of the various sectors and different processing operations.[58]

54 A comprehensive approach on personal data protection in the European Union – Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, European Commission, Brussels, 04.11.2010 COM (2010) 609/3, p. 12.

55 Proposed General Data Protection Regulation 2012, COM (2012) 11 final, Article 38.

56 Proposed General Data Protection Regulation 2012, COM (2012) 11 final, Article 38(1)(h).

57 Proposed General Data Protection Regulation 2012, COM (2012) 11 final, Article 38(2).

58 Proposed General Data Protection Regulation 2012, COM (2012) 11 final, Article 39.

10.3.4 International coordination and cooperation

It is to be noticed that personal data are transferred across national boundaries, both internal and external, at rapidly increasing rates.[59] Nationals should facilitate dialogue on how to enable cross-border enforcement of data privacy protection between countries. The EU and US have been working on this since the Safe Harbour Agreement in 2000. The SWIFT agreement allowing the sharing of EU citizens' bank data with the US authorities was also adopted in 2010. More recently in June 2012 the EU and US issued a Joint Statement on the negotiation of a EU-US Data Privacy and Protection agreement.[60] In need of international coordination of cross-border data privacy protection, more dialogues between countries have been gradually happening. For example, on 26 June 2013 the US Federal Trade Commission signed a Memorandum of Understanding with the Irish Privacy Enforcement Agency on Mutual Assistance in the Enforcement of Laws Protecting Personal Information in the Private Sector.[61] This is the first international mutual assistance agreement after the adoption of the Proposed General Data Protection Regulation in 2012. Article 45 of the Proposed General Data Protection Regulation 2012 encourages Member States to develop effective international cooperation mechanisms and international mutual assistance to facilitate the enforcement of legislation for the protection of personal data.[62]

In summary, it is an ongoing process of modernisation of existing rules due to the continuously rapid changes in technologies and the social, cultural and economic challenges of data privacy protection. The popularity of electronic services depends on users' trust and confidence which then relies on adequate levels of protection of data privacy and security. Without adaptable, organisational, technical and legislative measures, users may suffer financial loss and distress because they are at risk of their personal information being used other than in ways for which they have given specific permission.[63] The recent updated EU legal framework on data privacy protection intends to

59 Proposed General Data Protection Regulation 2012, COM (2012) 11 final, p. 6.

60 Joint Statement on the negotiation of a EU-US Data Privacy and Protection agreement by European Commission Vice-President Viviane Reding and US Attorney General Eric Holder, Brussels 21 June 2012, MEMO/12/474. Available at: http://europa.eu/rapid/press-release_MEMO-12-474_en.htm (last accessed 30 June 2013).

61 Memorandum of Understanding between the United States Federal Trade Commission and the Office of the Data Protection Commissioner of Ireland on Mutual Assistance in the Enforcement of Laws Protecting Personal Information in the Private Sector, 26 June 2013. Available at: http://www.ftc.gov/os/2013/06/130627usirelandmouprivacyprotection.pdf (last accessed 30 June 2013).

62 Proposed General Data Protection Regulation 2012, COM (2012) 11 final, Article 45(1).

63 Implementing the revised EU electronic communications framework: impact assessment, Department for Business, Innovation and Skills (BIS), September 2010. Available at: http://www.bis.gov.uk/assets/biscore/business-sectors/docs/i/10-1133-implementing-revised-electronic-communications-framework-impact.pdf (last accessed 30 June 2013), p. 6.

have a positive impact on the security conduct of data processing for both consumers and business organisations. The introduction of a duty on providers of electronic communications services to notify personal data breaches will be beneficial in improving consumer welfare as a result of potential reduced incidences of breaches of personal data. Such a notification system will be also beneficial to business organisations as a result of the potentially enhanced reputation as a result of implementing appropriate data breach notification measures, although there may be costs to adopting such measures. The Study on the Economic Benefits of Privacy-Enhancing Technologies (PETs): Final Report to the European Commission in July 2010 indicated that although there may be short-term costs with few tangible benefits, the longer-term impact on the business as a result of reputational gains would be significant.[64] National competent authorities endeavour to provide guidelines and instructions on data privacy protection to business organisations that collect and process personal data for the implementation of the new EC e-Privacy Directive and the assessment of the Proposed General Data Protection Regulation. Meanwhile, business organisations shall also take initiatives and develop technological approaches and tools that are compatible with the requirements of the new legislation, such as complying with the required standard of privacy-enhancing technologies (PETs), performing the duty of notification of personal data breaches without undue delay and taking possible measures and remedies to reduce or remove the risks according to the guidance of competent national authorities.

The success of the implementation of the data breach notification system requires the effects from both business organisations and competent national authorities. On one hand, business organisations shall learn the procedures of 'notification of the personal data breach' system; notify competent national authorities of data breach within 24 hours of detection where feasible and without undue delay; and maintain a detailed list of personal data breach information, effects and remedial actions taken for the verification of compliance by the competent national authorities. On the other hand, competent national authorities shall provide sufficient guidelines and instructions, which, in the author's view, should include standard forms and modalities of the notification system as well as adopt measures to prevent notification of data breaches involving unacceptable delay. As to the timeframe of notification of data breach, it is known that the time limit of such notification shall take into consideration not only the time limit that the provider is required to notify the personal data breach to the competent national authority in the first instance, but also the time period between notification to the competent national authority and notification to a subscriber or individual. There is a

64 Study on the Economic Benefits of Privacy-Enhancing Technologies (PETs): Final Report to the European Commission, DG Justice, Freedom and Security, July 2010, by London Economics, p. 74.

great necessity to clarify the timeframe of the notification of data breaches to a subscriber or individual due to the foreseeable complications once a subscriber or individual is informed.

With regard to the enforcement of the personal data breach notification system within Member States, it would be helpful if the strategy of the EU Comprehensive Approach 2010 could successfully build a common approach across the EU to remove the obstacle of the uncertainty of the timeframe of the personal data breach notification in the near future, so that multinational business organisations would only have to deal with one set of rules. Business organisations shall be encouraged to adopt the self-regulatory enforcement initiatives such as the trustmarks and privacy seal programmes to increase the efficiency of the enforcement of data privacy protection. After all, legislative and technological measures for data privacy protection shall strike a fair balance between the protection of the right to private life and the free movement of personal data.[65] It is also of great significance to protect data privacy rights without jeopardising business efficiency, market developments and technological innovations at a global level. Dialogues between countries shall be encouraged to develop international coordination and mutual assistance on the enforcement of data privacy protection.

65 Case C-518/07 *European Commission* v. *Germany*, European Court of Justice (Grand Chamber) 09 March 2010 [2010] 3 CMLR 3, paras 24 and 30.

11 Liability of Internet service providers: implementation of the notice and takedown (NTD) procedure[1]

11.1 The role of Internet service providers

It is a great challenge to define Internet service providers as there are many variations in titles, types and services. Internet service providers can be understood as intermediary service providers or online intermediaries, which provide transit, content, access and hosting services. Trusted service providers as discussed earlier may also be considered as Internet service providers that provide content signatures, authentication and certificates.

Online intermediaries play an important role in the information society, and as a result regulators have been taming the Internet through their use.[2] Online intermediaries not only provide electronic services but also assist in the enforcement of privacy data protection by adopting appropriate technical measures and performing the duty of the notification of data breaches to the competent authorities and subscribers. Moreover, online intermediaries are expected to implement the notice and takedown (NTD) procedures in response to the notification of illegal content, which includes privacy infringement content. It is feasible that incorporating the online dispute resolution (ODR) mechanism into the NTD system and merging the NTD system with the data breach notification mechanism may be a way forward to further promote the fairness and efficiency of consumer protection online.

The general liability of intermediary service providers was regulated in Articles 12–14 of the EC Directive on Electronic Commerce:

- Service providers are not liable for 'mere conduit' of the information transmitted without initiating the transmission, selecting the receiver of the transmission, and selecting or modifying the information contained in the transmission (Article 12).

1 Part of this chapter draws upon the author's publication: F. Wang (2012) 'Response to public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries', *Intellectual Property Forum*, 91: 93–8.

2 U. Kohl (2012) 'The rise and rise of online intermediaries in the governance of the Internet and beyond – connectivity intermediaries', *International Review of Law, Computers and Technology*, 26 (2–3): 185–210, at p. 185.

- Service providers are not liable for 'caching' the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request without modifying the information and interfering with the lawful use of technology and in compliance with conditions on access to the information and rules regarding the updating of the information, specified in a manner widely recognised and used by industry (Article 13).
- Service providers are not liable for 'hosting' the information stored at the request of a recipient of the service without actual knowledge of illegal activity or information and with an expeditious action to remove or disable access to such information upon obtaining such knowledge or awareness (Article 14).[3]

In addition, Article 15 of the EC Directive on Electronic Commerce specifies that service providers have no general obligation to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.[4]

This chapter provides commentaries on necessary measures to be considered for the establishment of NTD procedures in the EU with some reference to current development in the US regarding intellectual property (IP) rights, defamation and data privacy infringement.

11.2 Notice and action procedures in Europe

Hosting service providers can be categorised as one type of online intermediary. Giving a definition to the hosting service provider can be challenging as it is a relevant term. For example, the social network provider can be considered the hosting service provider if that social network provider owns and runs its server consisting of 'the storage of information provided'.[5] If another service provider leases server capacity to the social network provider, that service provider which leases server capacity should be considered as the hosting service provider. Hosting service providers have been actively engaging in the 'notice and takedown' practice regarding illegal online content. However, how far the responsibility and liability of hosting service providers should go remains a controversial issue.

The European Commission opened the Public Consultation on Procedures for Notifying and Acting on Illegal Content hosted by Online Intermediaries (hereafter 'the consultation') between 4 June 2012 and 5 September 2012

3 EC Directive on Electronic Commerce 2000, Articles 12–14.
4 EC Directive on Electronic Commerce 2000, Article 15(1).
5 EC Directive on Electronic Commerce 2000, Article 14.

(extended to 11 September 2012).[6] This consultation aimed to collect opinions on how to develop a clean and open Internet by reviewing the provisions under Article 14 of the EC Directive on Electronic Commerce, and was deemed to be another attempt at regulating the liability of online intermediaries after the publication of recent comments and reports on the enforcement of IP rights (the application of the EC Directive on Intellectual Property Rights Enforcement),[7] and the public consultation on the future of e-commerce and the implementation of the E-Commerce Directive.[8] The focal point of the consultation lay in questions on whether hosting service providers should have a procedure for notifying illegal content and what actions hosting service providers should take against illegal content.

'Notice and action' (N&A) procedures in this consultation are also known as 'notice and takedown' procedures (NTD) in other countries such as the UK and Hong Kong. Some other European official documents also use the wording 'notice and takedown', which can be found in the European reports and comments on e-commerce and IP rights enforcement. The N&A procedures are also called 'takedown procedures' or 'takedown notice' in the Digital Millennium Copyright Act in the US.[9] The NTD procedures are commonly understood as starting whenever someone notifies a hosting service about illegal content on the internet and concluding when an online intermediary takes down (i.e. blocks or deletes) the alleged illegal content.[10] The NTD procedures are deemed to be 'indispensable measures in the fight against the sale of Counterfeit Goods over Internet Platforms'.[11] It was also popularly used to fight against other IP rights infringement, defamatory content, terrorism related content, illegal online gambling, child abuse content, misleading advertisements

6 A Clean and Open Internet: Public Consultation on Procedures for Notifying and Acting on Illegal Content hosted by Online Intermediaries, 4 June 2012, European Commission. Available at: http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=noticeandaction (last accessed 30 June 2013).

7 Synthesis of the Comments on the Commission Report on the Public Consultation on the Application of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights, European Commission, July 2011. Available at: http://ec.europa.eu/internal_market/consultations/docs/2011/intellectual_property_rights/summary_report_replies_consultation_en.pdf (last accessed 30 June 2013).

8 Public Consultation on the Future of Electronic Commerce in the Internal Market and the Implementation of the Directive on Electronic Commerce (2000/31/EC), European Commission, 2010. Available at: http://ec.europa.eu/internal_market/consultations/2010/e-commerce_en.htm (last accessed 30 June 2013).

9 L. Pallas (2011) 'Deterring abuse of the copyright takedown regime by taking misrepresentation claims seriously', *Wake Forest Law Review*, 46: 745–82, at p. 745.

10 A Clean and Open Internet: Public Consultation on Procedures for Notifying and Acting on Illegal Content Hosted by Online Intermediaries, 4 June 2012.

11 Memorandum of Understanding on the sale of counterfeit goods over the internet (hereafter 'the MoU'), 4 May 2011, European Commission, Brussels. Available at: http://ec.europa.eu/internal_market/iprenforcement/docs/memorandum_04052011_en.pdf (last accessed 30 June 2013), Article 11.

or incitement to hatred or violence on the basis of race, origin, religion, gender, sexual orientation, etc.[12] In other words, the NTD procedures have been horizontally applied across a variety of legal subject matters.

However, such horizontal application have been implemented at various levels in different countries. In addition, each country has developed this mechanism with different strengths. For example, in the US there is debate over how to enhance fairness under such procedures. In the case of *Lenz* v. *Universal Music Corp.*,[13] the court introduced the fair use analysis under the takedown procedures in order to ensure the critical balance between a copyright owner's monopoly and the rights of the public.[14] That is, the copyright owner is required to conduct a fair use evaluation prior to issuing a takedown notice. In the EU, there is debate over how to improve effectiveness under such procedures. For example, the 'without undue delay' principle for data breach notification is introduced in the EC E-Privacy Directive.[15] The Proposed General Data Protection Regulation further enhances this principle by inserting Article 12(2) that 'the controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken'. Recital 67/Article 31 of the Proposed General Data Protection furthers the requirement that 'the controller should notify the breach to the supervisory authority without undue delay and, where feasible, within 24 hours. Where this cannot be achieved within 24 hours, an explanation of the reasons for the delay should accompany the notification'.[16] That is, a timescale for the 'notice and takedown' procedures has been considered a crucial measure to improve and enhance the effectiveness (and even fairness) of such procedures.

Despite the continuous development of the NTD procedures in the EU, member states are still facing one major challenging issue, that is the consistent or harmonised interpretation of the 'notice and takedown' procedures under the EU legislation such as the EC Directive on Electronic Commerce (2000/31/EC), the EC e-Privacy Directive (2009/136/EC), the EC Directive on IP Rights Enforcement (2004/48/EC), the EC Information Society Directive (2001/29/EC), etc. The cornerstone of the legislation regarding the

12 A Clean and Open Internet: Public Consultation on Procedures for Notifying and Acting on Illegal Content Hosted by Online Intermediaries, 4 June 2012, European Commission.

13 *Lenz* v. *Universal Music Corp.*, 572 F. Supp. 2d 1150, United States District Court for the Northern District of California, 8 August 2008.

14 K. O'Donnell (2009) 'Lenz v. Universal Music Corp. and the potential effect of fair use analysis under the takedown procedures of Section 512 of the DMCA', *Duke Law and Technology Review*, pp. 1–12, at p. 10.

15 F. Wang (2011) 'Personal data breach notification system in the European Union: interpretation of "without undue delay"', *European Business Law Review*, 6: 741–57, see generally.

16 Proposal for a Regulation of the European Parliament and the Council on the Protection of Individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), European Commission, Brussels, 25.1.2012 COM (2012) 11 final, 2012/0011 (COD).

'notice and takedown' procedures on the Internet is the provision of 'hosting' in the EC E-Commerce Directive (Article 14). It provides that:

> Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:
>
> (a) the provider does not have *actual knowledge* of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
> (b) the provider, *upon obtaining* such knowledge or awareness, *acts expeditiously* to *remove* or to *disable* access to the information.[17] (Emphasis added)

This defines the core factors for the determination of a hosting service provider's liability – 'actual knowledge', 'actions (remove/disable)' and 'manner (expeditiously)'. The wording of this provision is exactly the same as the relevant provision in the US Copyright Act,[18] though the EC Directive on Electronic Commerce is applicable to a wider scope of subject matters, known as a horizontal approach as discussed earlier. The meaning of the three core factors is rather open to dispute in practice and there is need for further clarification to avoid legal fragmentation and uncertainty for hosting service providers. It places reliance on standardising two components: the content of notification (formality and details of information) and the action against illegal content in response to notification.

11.2.1 Notification of illegal content

Hosting service providers may acquire 'actual knowledge' and 'awareness' of illegal activity or information upon the receipt of notification of illegal content. A notification of illegal content is usually required to be in a prescribed format to make the hosting service provider aware of alleged illegal content. In the EU, the Court of Justice of the European Union in the recent case of *L'Oréal and Others* v. *eBay* ruled that if notifications of allegedly illegal activities or information may turn out to be insufficiently precise or inadequately substantiated, hosting service providers may not be able to identify the illegality and take actions expeditiously to remove or disable access.[19] In the US, in *Hendrickson* v. *eBay Inc.*, it was held that it was inadequate to simply provide

17 EC Directive on Electronic Commerce, Article 14(1).
18 Copyright Act Title 17 USC (1976): see §512 in general.
19 Case C-324/09, *L'Oréal and Others* v. *eBay*, Court of Justice of the European Union, Luxembourg, 12 July 2011, para. 122.

eBay with the movie's title without specifying the eBay item number listings.[20] In other words, information regarding the alleged illegal content should be sufficiently precise and adequately substantiated for hosting service providers to gain 'actual knowledge' and 'awareness' of illegal activities.

To enhance this, in practice, some hosting service providers have voluntarily put in place technical mechanisms/systems for the 'notice and takedown' process. For example, it may be noted that eBay has developed an NTD system called 'VeRO' (Verified Rights Owner) – a filter program that is intended to provide IP owners with assistance in removing infringing listings from the marketplace. It requires that the complainant fill out the standard Notice of Infringement form specifying the allegedly infringing listings and infringed works complete with an original authorised signature and fax it to eBay.[21] Amazon also introduced its self-regulated 'notice and takedown' procedures to deal with rights infringements. Different from eBay, Amazon sets up separate formats for different rights infringement such as 'notice and procedure for notifying Amazon of defamatory content' and 'notice and procedure for making claims of right infringements'. The complainant will need to send to Amazon a printed and signed copy of the defamatory content notice after filling in a downloadable form.[22] Different from notification of defamatory content, the complainant is only required to fill in an online form regarding alleged infringements such as copyright and trademark concerns and click the 'submit' button to complete the report infringement process.[23] In the author's opinion, if hosting service providers impose exclusive offline notification methods such as fax and post, it may not appear to be user-friendly taking into account the common use and popularity of e-mail and other electronic communications in the information society. As the consultation rightly pointed out, the EC Directive on Electronic Commerce has not addressed the requirements regarding the means of communication, format and content of notification, and although the Court of Justice of the European Union (CJEU) in *L'Oréal and Others* v. *eBay* indicated that a notice should be sufficiently precise or adequately substantiated to have effect, the court has not indicated the requirements of meeting such purpose.[24] In the author's opinion, making the 'notice and takedown' procedures as user-friendly as possible is of

20 *Hendrickson* v. *eBay Inc.*, 165 F Supp 2d 1082 (CD Cal 2001).

21 eBay VeRo Program information. Available at: http://pages.ebay.co.uk/vero/notice.html (last accessed 30 June 2013).

22 Notice and Procedure for Notifying Amazon of Defamatory Content. Available at: http://www.amazon.co.uk/gp/help/customer/display.html?nodeId=1040616#defame (last accessed 30 June 2013).

23 Notice and Procedure for Making Claims of Right Infringements – Report Infringement. Available at: https://www.amazon.co.uk/gp/help/reports/infringement (last accessed 30 June 2013).

24 A Clean and Open Internet: Public Consultation on Procedures for Notifying and Acting on Illegal Content Hosted by Online Intermediaries, 4 June 2012, p. 10.

fundamental importance as this is one of the most effective ways to promote the usage of such a system to protect users' and other rights holders' rights and at the same time minimise the possibility of the avoidance of responsibilities by hosting service providers. Thus, ideally, this principle should be made compulsory to hosting service providers by regulators. It is incontrovertible that having a fair procedure in place by means of which users can easily notify hosting service providers of illegal content will not only boost users' confidence in using online marketplaces but also help service providers gain a good reputation. Accordingly, proposals for the possible interpretation of the requirements of 'sufficiently precise or adequately substantiated' may be that:

- a notice should be allowed to be submitted by electronic means;
- a notice should contain details of the sender but hosting service providers must not disclose the sender's personal details to other parties without informed consent except for crime investigation authorities;
- a notice should specify the precise location and details of the alleged illegal content including but not limited to a URL, itemised number and detailed description of the alleged illegal nature of the content; and
- a notice should be accepted by the hosting service provider regardless of whether the user can provide proof or evidence that the content provider (other rights holder) could not be contacted or the content provider was contacted first but did not act, because acceptance to notification should be treated as a responsibility of hosting service providers to users so as to avoid diminishing the function of the NTD system.

11.2.2 Action against illegal content

In the EU, once the notified illegal content and its nature of infringement have been confirmed, the hosting service provider is expected to act 'expeditiously' to remove or disable access to information according to the EC Directive on Electronic Commerce.[25] In the US, the responsible service provider is also required to respond 'expeditiously' to a notice (e.g. copyright infringement).[26] However, there is no clear definition of 'expeditiously' or of the specific actions required so as to 'remove or disable access'. In practice, as the consultation indicated, some service providers may send the notice party a confirmation of receipt when they receive a notice and inform the notice party when the requested action has been taken.[27] This measure bears some similarity to that of the 'without undue delay' principle for data breach notification discussed earlier. For example, it was proposed that the controller shall inform the data

25 EC Directive on Electronic Commerce, Article 14(1).
26 Copyright Act Title 17 USC (1976): §512(b)(2)(E) and §512(c)(1)(c).
27 A Clean and Open Internet: Public Consultation on Procedures for Notifying and Acting on Illegal Content hosted by Online Intermediaries, 4 June 2012, European Commission, p. 13.

subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken.[28] Likewise, the controller should also notify the breach to the supervisory authority without undue delay and where feasible within 24 hours.[29] It is understood that regulatory explanation, taking into account judicial clarification, should be in place to enhance the consistent, efficient and harmonised actions against illegal content by hosting service providers. In the author's opinion, hosting service providers should be required to:

1. send a confirmation of receipt to the notice parties (i.e. the notice providers or rights holders) when they receive a notice (by an automated e-mail confirmation instantaneously or by other means within 24 hours);
2. consult the notice parties of alleged illegal content (for additional information and clarification) within 24 hours after the confirmation of receipt of the notice;
3. consult the users/clients (i.e. the online content writer or information/content provider) concerning the allegation of content illegality (the so-called 'counter-notice') within 24 hours simultaneously; and
4. inform both the notice parties and users/clients of any action that has been taken without undue delay depending on circumstances.

This can be deemed 'a four-step approach' for the N&A procedure. It is unavoidable that there may be difficulties in implementing this four-step approach due to various expectations such as efficiency, fairness and appropriateness. The debate is likely to fall into two areas: one is the area regarding the adoption of the counter-notice system and the other is the area concerning the appropriate actions (i.e. remove or disable access) and the timeframe of such actions by the hosting service provider.

In the author's view, the counter-notice system should be recommended for the reasons that: firstly, lawsuits take a long time and the results may not be desirable in an online defamation case;[30] and secondly, users' rights are as important as other rights holders' rights (i.e. copyright holders' rights). Taking into account the balance that needs to be made, the counter-notice system has been introduced in many countries such as Finland, Lithuania, Poland, Germany and the US.[31] The counter-notice system allows counter parties to dispute or deny the infringement alleged by the complainant and request online intermediaries reinstate the material or cease disabling access to the

28 Proposed General Data Protection Regulation 2012, Article 12(2).

29 Proposed General Data Protection Regulation 2012, Recital 67 and Article 31.

30 *McGrath* v. *Dawkins & Others* [2012] EWHC B3 (QB) (England, High Court, 30 March 2012).

31 G. Spindler, G. M. Riccio, and A. Perre, 'Study on the liability of Internet intermediaries' (Markt/2006/09/E Service Contract ETD/2006/IM/E2/69), 12 November 2007. Available at: http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf (last accessed 30 June 2013), p. 16.

material or activity. For example, in the US, if the complainant does not inform the service provider that he/she has filed an action seeking for a court action after 10 to 14 days upon the receipt of a counter-notification, the service provider may reinstate the alleged materials.[32] Such a measure has also been considered in other countries; for instance, Hong Kong also intends to introduce the counter-notice system in its Copyright (Amendment) Bill 2011.[33] Due to the conflicting interests between various parties and the public, having a counter-notice system in place will not only balance the rights between the users and other rights' holders but also best prevent unjustified notifications.

With regard to the issue concerning the appropriate actions (i.e. remove or disable access) and the timeframe of such actions, it is even more complex as it is intertwined with other issues horizontally such as criminal investigations from law enforcement authorities and diverse regulatory requirements of data privacy protection, IP rights enforcement, defamatory content, online gambling, consumer protection and others. Moreover, the appropriate actions and timeframe should be clearly considered at each stage of communications throughout the four-step process. For example, in the US, the safe harbour provisions do not require the service provider to notify the user/client for the allegedly infringing material before it has been removed, but the service provider must promptly notify the user/client after the material is removed and the user/client can then decide on its actions (i.e. giving a counter-notice and/or filing a lawsuit).[34] In the EU, the practice is similar to that in the US. As a result, the hosting service provider will take down the content immediately after receiving a notice and will only be obliged to put it back online after receiving a counter-notice.[35] However, such a measure leaves the hosting service provider with the responsibility to assess the legitimacy of the alleged information, content or statement. So when the judgment goes wrong, the hosting service provider may disable or take down legal content. If the rights holder (the notice provider) takes a step further and files a lawsuit against the user/client, the alleged materials will remain disabled, blocked or removed at least until the court makes the final decision.

The speed of taking down the alleged materials (either legal content or illegal content) may cause various effects. In other words, at which stage the hosting service provider is required to disable or remove access is going to affect speed and as a consequence cause different effects. This is going to be an ongoing debate from an economic perspective, because Internet users

32 Copyright Act Title 17 USC (1976): see §512(g)(2)(c).

33 Copyright (Amendment) Bill 2011, Section 88D. Available at: http://www.legco.gov.hk/yr10-11/english/bills/b201106033.pdf (last accessed 30 June 2013).

34 Copyright Act Title 17 USC (1976): see §512(g)(2)(a) and Frequently Asked Questions (and Answers) about DMCA Safe Harbour. Available at: http://www.chillingeffects.org/dmca512/faq.cgi (last accessed 30 June 2013).

35 G. Spindler, G. M. Riccio and A. Perre (2007) 'Study on the liability of Internet intermediaries' (Markt/2006/09/E Service Contract ETD/2006/IM/E2/69), 12 November, p. 16.

may suffer from lost benefits or profits and even economic damages as a result of the alleged materials being wrongly taken down, and so may the rights holders, who can claim the loss of profits for their work being illegally copied. From a social security perspective, certain types of damages can be magnified or pretty soon become out of control if the hosting service provider does not take action to disable or remove material immediately, e.g. in the case of live video streaming or subject matter involving threats to national security. Nevertheless, from a general human rights perspective, both users and rights holders should be given an equal opportunity to express their views on the alleged infringing materials before the materials are permanently taken down, provided that the alleged materials do not pose an immediate threat to social security and the public interest.

This leads to the next controversial issue which concerns the appropriate actions to be taken with regard to whether the hosting service provider should disable access in the first instance without permanently removing, taking down or deleting the content. Firstly, certain rights (such as IP rights) are protected within the territory where such rights are registered. Permanently removing the content may hamper the users' rights to use the content in another jurisdiction. Secondly, certain concepts such as privacy and defamation are related to culture and democracy respectively, which the hosting service provider may not be in a position to make a judgment on in terms of the legitimacy of the content. Thirdly, removing the alleged illegal materials may prevent law enforcement authorities from further analysing them and investigating crimes when necessary. Lastly, the hosting service provider should be technically in a position to remove exclusively the notified illegal content when several providers host the same content on a particular website.[36] It should also be noted that removing materials from a search engine does not necessarily remove them from the Internet, which may cause further complication and difficulty in locating the alleged materials afterwards for the purpose of criminal investigations.[37] After all, the N&A procedure should be realistic on the matter whether the hosting service provider has the capability to take the responsibility to assess the legitimacy of the alleged information, content or statements. In order to ensure fairness and security, the hosting service provider should be obliged to notify the competent authorities without undue delay when there is any doubt on whether the alleged information, content and statements may constitute a severe breach of the social security and public interest. In any event, suspicious alleged illegal materials should be disabled in the first instance when the hosting service provider receives a notice, though the system may be abused by the notice provider when the

36 A Clean and Open Internet: Public Consultation on Procedures for Notifying and Acting on Illegal Content Hosted by Online Intermediaries, 4 June 2012, p. 15.

37 J. Urban and L. Quilter (2005–6) 'Efficient process or chilling effects – takedown notices under Section 512 of the Digital Millennium Copyright Act', *Santa Clara Computer and High Technology Law Journal*, 22: 621–93, at p. 626.

underlying purpose of such notice is to prevent others from using lawful materials to gain dominant position or other benefits. It is understood that this can be protected by imposing sanctions to such abuse.

After all, the use of the wording 'notice and action' procedures (the N&A procedures) in the consultation instead of 'notice and takedown' procedures (the NTD procedures) may be well justified in the sense that the 'notice and takedown' procedures not only comprise 'notice' and 'takedown' actions but also involve other actions such as counter-notice, evaluation and other remedies as discussed above, though NTD ('notice and takedown') has become a universal common name for such procedures.

What the N&A procedures should be depends on what the purposes of having such procedures in place are. It is known that the original purpose of the NTD procedures was debatable and such purposes should be now justified before the regulatory design. The intended role of hosting service providers (such as gatekeepers, guardians or even mediators, etc.) will inevitably reflect on the scope of their responsibility and liability. Whichever role regulators may decide on for hosting service providers, due process and fair use (fairness) should be considered as the two fundamental principles for the N&A procedure for two reasons: (1) from the users' perspective, the adoption of such procedures may be for the creation of chilling effects and to suppress freedom of expression or communications; and (2) from the Internet service providers' perspective, the deployment of such procedures is to gain exemption from liability for the hosting of illegal content. However, according to the issues raised in the consultation, it appears that the system of the N&A procedures may be progressed to serve as a protocol to strike a balance between protecting users' and various rights holders' rights and promoting the role of Internet service providers in response to the rapid development of social networking and other forms of electronic communications.

Part III Summary

Electronic signatures and authentication, as a means of providing safety, reliability and integrity in e-transactions, play an important role in e-commerce as they create trust and confidence. With the rapid uptake of electronic commerce, predictably, there has been a rush to enact laws and legislative measures. These laws may suffer from two fundamental problems. First, the fast-changing nature of technologies has the potential to render any legislation redundant within a short period of time. In addition, national laws are inadequate for governing what is truly a global issue. Regulation poses further threats in that it risks stifling electronic commerce if it is unduly burdensome.[38] A large number of supplementary legislative measures have been introduced and adopted without thorough consideration in the EU and China since 2006 which may overwhelm a clear and constructive legal order. In contrast, international organisations and the US have been reluctant to enact new laws since 2006, though efforts have been made in interpreting existing legal concepts to adapt them to the new high-tech environment and to facilitate international cooperation and implementation.

Trust and security are now, more than ever, critical issues in doing business, whether online or in the paper world. The development of global harmonised legislative standards concerning electronic signatures and authentication, data privacy protection and information security becomes ever-increasingly vital to facilitate international commerce in the digital economy. Undoubtedly legal certainty and predictability can only be achieved through the harmonisation of international, regional and national legislation and practices.

Though international, regional and national laws have reduced legal barriers by recognising the effectiveness of forming a contract and giving a signature by electronic means in principle, there are various constraints on the recognition of the interoperability regarding technical and legislative standards which lead to inconsistent results for the determination of the effectiveness of electronic contracts and signatures at national, regional and international levels. An establishment of international trust service mechanisms through constructively standardising the conditions, liabilities and remedies of certification authorities may be of great necessity to remove the obstacles to the development of reliable electronic commerce.

It is notable that data privacy protection also relies on secure and reliable electronic signatures and authentication. Although the EU, US, China and international organisations have acknowledged common principles of data privacy protection, national and regional substantive laws take different approaches in regulating the relevant issues. For example, the EU legislation

38 C. Swindells and K. Henderson (1998) 'Legal regulation of electronic commerce', *Journal of Information, Law and Technology*, 3, available at: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1998_3/swindells (last accessed 30 June 2013).

aims more at protecting individual privacy rights, while the US and international guidelines gear towards promoting the free flow of cross-border data for the development of the global economy. There is one aspect in common: they all make efforts to balance individuals' privacy rights, market developments and technological innovations in order to promote the global digital economy. The trustmark programme, provided by a trusted third party certifying the quality of merchants' data privacy, together with the notice and takedown mechanism, should be deemed to be one of the most effective approaches in enhancing users' trust and confidence in online interaction and transactions.

This page intentionally left blank

Part IV
Dispute Resolution

This page intentionally left blank

12 Resolving electronic commercial disputes

Businesses, through the use of the Internet, can enter into electronic contracts of sale with other businesses located in different countries. Computing technologies make it possible to download intangible/digitised goods onto computers without the need of physical delivery. This has undoubtedly improved economic efficiency, competitiveness and profitability. Resolving cross-border disputes concerning electronic transactions is inevitably more complicated than in a paper-based environment, because connecting factors such as the place of domicile, the place of business and the place of performance are difficult to define on the Internet. The determination of Internet jurisdiction and applicable law has been greatly challenged when online contracting or transactions are executed in several places as it raises the difficulty of ascertaining the principal place of performance.

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 (hereafter 'the UN Convention') do not contain any provisions on jurisdiction or choice of law, 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 to 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. In the EU, the EC Directive on Electronic Commerce (Recital 23 and Article 1(4)) also does not establish any additional rules on private international law

1 UNCITRAL Model Law on Electronic Commerce, on the report of the Sixth Committee (A/51/628), 16 December 1996, Article 15; and also the UN Convention on the Use of Electronic Communications in International Contracts, (hereafter 'the UN Convention') 2005, Article 10.

2 The UN Convention 2005, Article 6.

with regard to jurisdiction and choice of law.[3] Likewise, in China and the US there is no particularised Internet jurisdiction and choice of law legislation. In absence of subject specific legislation for Internet jurisdiction and choice of law, there is a need for the interpretation and implementation of general traditional conflict of law rules for Internet-related disputes, taking into consideration the features of electronic communications and their relevant regulations. Arguably alternative dispute resolution (ADR), in particular online dispute resolution (ODR), may be deemed to be one of the most efficient and appropriate methods to resolve certain types of Internet-related disputes.

12.1 Internet jurisdiction[4]

It is widely recognised that jurisdiction is one of the main topics within the scope 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 jurisdiction. In the absence of particularised national, regional and international legislation concerning Internet jurisdiction, it will depend on the courts to interpret the existing jurisdictional rules for the determination of the effectiveness of jurisdiction clauses concluded by electronic means and competent courts to resolve Internet-related disputes. 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 matter infringements, occurred. Whether the traditional rules of jurisdiction can still be sufficient to determine Internet jurisdiction has been debated and assessed in recent years.

12.1.1 EU rules applied in cyber jurisdiction

In the EU, jurisdiction concerning civil and commercial matters is governed by the Brussels I Regulation (EC No. 44/2001),[5] which replaced the 1968 Brussels Convention. The Brussels I Regulation is deemed to be:

> a highly successful instrument, which has facilitated cross-border litigation through an efficient system of judicial cooperation based on comprehensive

3 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 'the EC Directive on Electronic Commerce'), Recital 23 and Article 1(4).

4 Part of the EU and US sections draws upon the author's publications: F. Wang (2008) 'Obstacles and solutions to Internet jurisdiction: a comparative analysis of the EU and US laws', *Journal of International Commercial Law and Technology*, 3 (4): 233–41, and F. Wang (2013) 'Jurisdiction and cloud computing: further challenges to Internet jurisdiction, *European Business Law Review*, 24 (5).

5 Council Regulation on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matter (hereafter the 'Brussels I Regulation'); see Council Regulation (EC) No. 44/2001, 22 December 2000, OJ L 012, 16 January 2001, p. 1. Available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_012/l_01220010116en00010023.pdf (last accessed 30 June 2013).

> jurisdiction rules, coordination of parallel proceedings, and circulation of judgments. The system of judicial cooperation laid down in the Regulation has successfully adapted to the changing institutional environment (from intergovernmental cooperation to an instrument of European integration) and to new challenges of modern commercial life.[6]

This was endorsed 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 cooperation between Member States and its achievement in facilitating cross-border litigation cannot be undermined. However, it is probably arguable whether or not the Brussels I Regulation has successfully adapted to new challenges of modern commercial life, in particular new judicial issues on Internet-related cases, as Article 23(2) of the Brussels I Regulation is the only rule that explicitly acknowledges agreements by electronic means. On 21 April 2009 the Green Paper accompanying the Commission's Report launched 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
Question 8: other issues.

The main purpose of the eight consultation questions is to collect opinions on how to remove obstacles to a free circulation of judgments, how to enhance certainty of cross-border jurisdiction relating to one of the parties domiciled

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 April 2009, COM (2009) 174 final, Commission of the European Communities. Available at: http://www.ipex.eu/ipex/cms/home/Documents/doc_COM20090174FIN (last accessed 30 June 2013).

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 April 2009, COM (2009) 175 final, Commission of the European Communities. Available at: http://www.ipex.eu/ipex/cms/home/Documents/doc_COM20090175FIN (last accessed 30 June 2013).

8 *Lis pendens:* a pending lawsuit. In the EU, the *Lis pendens* rule requires that where proceedings involving the same cause of action and between the same parties are brought in the courts of different Member States, any court other than the Court first seised shall of its own motion stay its proceedings until such time as the jurisdiction of the court first seised is established.

in a third country rather than in a Member State, and how to avoid parallel proceedings in different Member States. Questions 2, 3 and 5 are connected and interact, 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 indirectly point to the query of the determination of Internet jurisdiction, the revision of the Brussels I Regulation shall ensure smooth operation in the international legal order, which will subsequently reflect on facilitating Internet jurisdiction.

Following the review of the Brussels I Regulation, on 6 December 2012 the Brussels I Regulation (Recast) was finally adopted by the European Parliament and the Council.[9] The Brussels I Regulation (Recast) 2012 is deemed to 'make the circulation of judgments in civil and commercial matters easier and faster within the Union'.[10] For example, the Brussels I Regulation (Recast) abolishes the *exequatur* procedure. The new *lis pendens* rules (Articles 29 to 34) contain provisions that 'allow the courts of a member state, on a discretionary basis, to stay the proceedings and eventually dismiss the proceedings in situations where a court of a third state has already been seized either of proceedings between the same parties or of a related action at the time the EU court is seized.'[11] This is to improve efficiency of dealing with cases from the same parties or related actions. Article 31(2)(3) of the Brussels I Regulation (Recast) 2012 as an addition to Article 29 of the Brussels I Regulation specifies that 'any court of another Member State shall stay the proceedings until such time as the court seised on the basis of the agreement declares that it has no jurisdiction under the agreement'.[12] This is to ensure that exclusive jurisdiction clauses can take effect without delay.[13]

Choice of court clauses or agreements

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

9 Regulation (EU) No. 1215/2012 of the European Parliament and of the Council 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast), OJ L 351/1, 20 December 2012 (hereafter 'the Brussels I Regulation (Recast) 2012'). Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:351:0001:0032:En:PDF (last accessed 30 June 2013).

10 Recast of the Brussels I Regulation: Towards Easier and Faster Circulation of Judgments in Civil and Commercial Matters within the EU, PRES/12/483, 6 December 2012. Available at: http://europa.eu/rapid/press-release_PRES-12-483_en.htm#PR_metaPressRelease_bottom (last accessed 30 June 2013).

11 PRES/12/483, 6 December 2012.

12 The Brussels I Regulation (Recast) 2012, Article 31(2)(3).

13 Brussels Office Law Reform Update Series: EU Civil Law, the Law Societies' Joint Brussels Office, April 2013. Available at: http://international.lawsociety.org.uk/files/CivilLawReformUpdate_April2013.pdf (last accessed 30 June 2013).

court or the courts of a named country.[14] On 1 April 2009 the European Council signed on behalf of the European Community the Hague Convention on Choice of Court Agreements[15] concluded on 20 June 2005 (hereafter 'the Choice of Court Convention').[16] The Choice of Court Convention applies to exclusive choice of court agreements concluded in civil or commercial matters with an international element.[17] So when the EU accedes to the Choice of Court Convention, the European Commission shall clarify the meaning of 'international cases' 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 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, suppose 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.[18] 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'.[19] 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 does not

14 J. H. C. Morris, D. McClean and K. Beevers (2005) *The Conflict of Laws*, 6th edn (London: Sweet & Maxwell), p. 87.

15 Convention of 30 June 2005 Choice of Court Agreements (hereafter 'the Choice of Court Convention'), The Hague. Available at: http://www.hcch.net/index_en.php?act=conventions.text&cid=98 (last accessed 30 June 2013).

16 Hague Convention Status Table. Available at: http://www.hcch.net/index_en.php?act=conventions.status&cid=98 (last accessed 30 June 2013).

17 The Choice of Court Convention 2005, Article 1(1).

18 *W.H. Martin Ltd* v. *Feldbinder Spezialfahzeugwerke GmbH* [1998] I.L.Pr. 794.

19 Case C–159/97 *Castelletti* v. *Trummpy* [1999] ECR I-1597.

prevent parties from changing their decisions.[20] In addition, Article 23(3) of the Brussels I Regulation 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. The courts of the other members shall have no jurisdiction over the disputes unless the chosen court or courts have declined jurisdiction.

In contrast, Article 25(1) of the Brussels I Regulation (Recast) replaces Article 23(1)(3) of the Brussels I Regulation and removes the distinction between parties domiciled and non-domiciled in the EU. It states that:

> If the parties, *regardless of their domicile*, have agreed that a court or the courts of a Member State are to have jurisdiction to settle any disputes which have arisen or which may arise in connection with a particular legal relationship, that court or those courts shall have jurisdiction, unless the agreement is *null and void* as to its substantive validity under the law of that Member State. Such jurisdiction shall be exclusive unless the parties have agreed otherwise.[21]

It should also be noted that the Brussels I Regulation (Recast) finally incorporates the condition of 'null or void' from the Choice of Court Convention into its new rule of determining the validity of exclusive jurisdiction agreements. This significantly improves the consistency in determination of a valid choice-of-court clause with the Choice of Court Convention. In the author's view, the introduction of 'null and void' for determining the validity of a choice of court agreement would enhance the effectiveness of exercising party autonomy on choice of court agreements and giving priority to the forum chosen by the parties. The introduction of the principle of 'null and void' to the Brussels I Regulation is not intended to cause further complication in assessing the material validity of the parties' agreements as it should have been according to domestic law, but to produce harmonised standards between Member States. Indeed, to maximise the positive effects and the efficient implementation of the 'null and void' principle, the European Commission may need to give additional guidance and explanatory notes. One of the feasible solutions to enhance harmonised standards could be by illustrating standardised examples of valid exclusive choice of court agreements without rigidly restricting the validity to particular wording for such agreements.[22]

Furthermore, the Brussels I Regulation (Recast) adds Article 25(5) clarifying that 'an agreement conferring jurisdiction which forms part of a contract shall be treated as an agreement independent of the other terms of the contract.'

20 *Sinochem* v. *Mobil* [2000] 1 Lloyd's Rep 670.

21 The Brussels I Regulation (Recast) 2012, Article 25(1).

22 F. Wang (2013) 'Regulation of Internet jurisdiction for B2B commercial transactions: EU and US compared', in P. Jurčys, P. F. Kjaer and R. Yatsunami (eds), *Regulatory Hybridization in the Transnational Sphere* (Leiden: Brill), pp. 99–124, at p. 111.

This affirms that invalidity of the contract or other terms does not affect the effectiveness of a jurisdictional clause or agreement, which should be considered to be 'independent'.

With regard to the effectiveness of jurisdictional clauses or agreements concluded by electronic means, Article 25(2) of the Brussels I Regulation (Recast) remains the same wording as Article 23(2) of the Brussels I Regulations and recognises that 'any communication by electronic means which provides a durable record of the agreement shall be equivalent to writing'.[23]

It means that agreements exchanged over the network as a secured Word document (i.e. a read-only document or document with entry password), or concluded by email and clicking an 'I agree' button may fall within the scope of Article 23(2) of the Brussels I Regulation or Article 25(2) of the Brussels I Regulation (Recast). Such electronic exclusive jurisdiction agreements must be available to read, download and reprint. In addition, such agreement will also need to meet certain formal criteria of contractual agreements such as the mutual consent of the parties. The approval of parties' mutual consent will be complicated for an electronic contract automatically concluded by the automated computing system without any human interaction. Under such circumstances, evidence must be established to show that the parties have agreed in writing to use an automated choice of court agreement concluded by the system itself; such practices have been established between parties themselves; or parties have been aware of such usage that is commonly accepted in international trade or commerce, especially in the particular trade or commerce concerned. This can be referred to Article 23(1) of the Brussels I Regulation (now Article 25(2) of the Brussels I Regulation (Recast)) that an exclusive choice of court agreement conferring jurisdiction shall be either:

(a) in writing or evidenced in writing; or
(b) in a form which accords with practices which the parties have established between themselves; or
(c) in international trade or commerce, in a form which accords with a usage of which the parties are or ought to have been aware and which in such trade or commerce is widely known to, and regularly observed by, parties to contracts of the type involved in the particular trade or commerce concerned.

It is arguable that a choice of court agreement incorporated into the clickwrap agreement will be valid. In the case of *Tilly Russ and Ernest Russ* v. *NV Haven- & Vervoerbedrijf Nova and NV Goeminne Hout* (known as the *Tilly Russ* case), the ECJ held that a jurisdiction clause contained in the printed conditions on a bill of lading satisfies the conditions laid down by Article 17 of the Brussels

23 The Brussels I Regulation 2001, Article 23(2); and also the Brussels I Regulation (Recast) 2012, Article 25(5).

Convention (now Article 23 of the Brussels I Regulation and Article 25 of the Brussels I Regulation (Recast)).[24] In the case of *Estasis Salotti di Colzani Aimo e Gianmario Colzani s.n.c.* v. *Rüwa Polstereimaschinen GmbH*, the court ruled that to meet the requirement of 'in writing or evidenced in writing', parties must sign the front of the contract inserting an express reference to general conditions that are on the back with a jurisdiction clause.[25] Such reference must be clear, have been communicated to other contracting parties and can be checked by a party exercising reasonable care.[26]

With the employment of cloud computing, when automated commercial transactions involve various places of performance and data are processed in different data centers, parties can restrict the location of data centers by agreeing upon certain data being stored and processed in certain data centers. However, this solution is only feasible when such service contract is constructed between business entities with more or less equal negotiation powers. Even if business entities achieve such limitation to data location, this may jeopardise the full advantages of using cloud computing infrastructure in organisations. It is possible that jurisdictional agreements can be automatically formulated according to a series of written codes/rules in automated computing systems. For example, the formula can be created as:

> Each block of service within one contract of service should be restricted to one data center only and the location of such data centre should be at the closest place to the services provided. Parties should bring the lawsuits to the courts of the place where, under the contract, the services were provided or should have been provided.

No matter which methodology of formula is chosen, parties can also increase the predictability of the validity of automated jurisdiction agreements by inserting a statement in the main service contract of using automated trading systems such as 'the jurisdiction clauses that are automatically generated by automated trading systems should be valid and exclusive, provided that such choices are based on the recipient's indication of the place of performance in the systems.' Alternatively, it is also possible to establish the recognition of such trade customs in the field of automated trading systems by the endorsements of local, regional or state chambers of commerce. Although the validity of automated choice of court clauses is recognised in principle, the automated insertion of choice of court agreements for data protection in the cloud-based environment may provide less feasible protection for cloud

24 *Tilly Russ and Ernest Russ* v. *NV Haven- & Vervoerbedrijf Nova and NV Goeminne Hout*, Judgment of the Court of 19 June 1984, Case 71/83.

25 *Estasis Salotti di Colzani Aimo e Gianmario Colzani s.n.c.* v. *Rüwa Polstereimaschinen GmbH*, Case 24/76 [1976] ECR 1931, para. 10.

26 [1976] ECR 1931, paras 12–13.

users (when disputes concerning data breach occur) than those for the sale of digital goods (when disputes concerning the delivery or quality of goods occur). It may be more predictable and protective to choose a selected list of courts for data protection in service-oriented computing in the cloud-based environments between cloud providers, cloud customers and cloud users upfront in the main service contract.[27]

In the situation where there are complex automated transactions comprising a number of agreements, most of which contain non-exclusive jurisdiction clauses in favour of one court but one agreement contains an exclusive jurisdiction clause in favour of the other court, it is necessary for the court to ascertain the parties' intentions. The recent English case *UBS Securities LLC* v. *HSH Nordbank AG* concerning jurisdiction clauses in complex financial transactions suggested that it was the dispute resolution clause 'at the commercial centre of the transaction' which was intended to govern such disputes.[28] In this case, the exclusive English jurisdiction clause in the Dealer Confirmation only related to technical banking disputes but not to the heart of the transaction, whereas the non-exclusive New York jurisdiction clauses applied at the commercial centre of the transaction.

If there is no exclusive jurisdiction clause or agreement, the courts will determine the jurisdiction of Internet-related civil and commercial issues according to three main types of traditional jurisdiction rules in the Brussels I Regime: 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.[29] Under Article 2 of the Brussels I Regulation (now Article 4 of the Brussels I Regulation (Recast)), persons domiciled in a Member State shall, whatever their nationality, be sued in the courts of that state. Furthermore, the domicile rules within the Brussels I Regulation govern the domicile of individuals[30] and of corporations.[31] 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.[32] Article 59(1) of the

27 F. Wang (2013) 'Jurisdiction and cloud computing: further challenges to Internet jurisdiction', *European Business Law Review*, 24 (5).

28 [2009] EWCA Civ. 585.

29 The Brussels I Regulation 2001, Article 2.

30 The Brussels I Regulation 2001, Articles 2 and 59; and also the Brussels I Regulation (Recast) 2012, Articles 4 and 62.

31 The Brussels I Regulation 2001, Article 60; and also the Brussels I Regulation (Recast) 2012, Article 63.

32 J. Fawcett, J. Harris and M. Bridge (2005) *International Sale of Goods in the Conflict of Laws* (New York: Oxford University Press), p. 511.

Brussels I Regulation (now Article 62(1) of the Brussels I Regulation (Recast)) 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) of the Brussels I Regulation (now Article 63(1) of the Brussels I Regulation (Recast)) lays down that for the purposes of the Brussels I Regulation a company or other legal person or association of natural or legal persons is domiciled at the place where it has (1) its statutory seat or (2) its central administration or (3) its principal place of business.

The domicile rule also applies to B2C commercial transactions that 'a consumer may bring proceedings against the other party to a contract either in the courts of the Member State in which that party is domiciled or, regardless of the domicile of the other party, in the courts for the place where the consumer is domiciled', and 'proceedings may be brought against a consumer by the other party to the contract only in the courts of the Member State in which the consumer is domiciled'.[33] Although the Brussels I Regulation (Recast) adds the wording 'regardless of the domicile of the other party', it does not change the original meaning provided by the Brussels I Regulation but makes it clearer.

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.[34] 'The location of the parties'[35] is defined as 'a party's place of business' in the UN Convention.[36] 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.[37] 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'.[38] In the author's view, in the online environment the determination of the person's habitual residence regarding B2B contracts for the sale of goods should be the same as that in the traditional environment, that is 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

33 The Brussels I Regulation 2001, Article 16; and also the Brussels I Regulation (Recast) 2012, Article 18.

34 J. Fawcett, J. Harris and M. Bridge (2005) *International Sale of Goods in the Conflict of Laws* (New York: Oxford University Press), p. 511.

35 The UN Convention 2005, Article 6.

36 The UN Convention 2005, Article 6(1).

37 The UN Convention 2005, Article 6(3); and also the UNCITRAL Model Law on Electronic Commerce 1996, Article 15(4)(b).

38 The UNCITRAL Model Law on Electronic Commerce 1996, Article 15(4)(b).

of business is that which has the closest relationship to the relevant contract.[39] The closest connecting factors are those that occur before or at the conclusion of the contract.[40] In the author's opinion, these factors have no difference from the offline world, which should 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 (now Article 7 of the Brussels I Regulation (Recast)) derogates from the general principle contained in Article 2 of the Brussels I Regulation, 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) of the Brussels I Regulation (now Article 7(1) of the Brussels I Regulation (Recast)), deals with matters relating to a contract. This general rule does not apply to insurance, consumer and employment contracts.[41]

How to ascertain 'the place of performance of the obligation in question'[42] is the focal point of how to determine jurisdiction. The place of performance, according to Article 5(1)(b) of the Brussels I Regulation (now Article 7(1)(b) of the Brussels I Regulation (Recast)), is the place of delivery of goods (or where they 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 makes no difference from a paper-based contract when the contract itself involves physical delivery of goods. The difficulty in applying Article 5(1) (now Article 7(1) of the Brussels I Regulation (Recast)) lies on the interpretation of whether multiple places of delivery are within the scope of this provision.

Unfortunately what Article 5(1)(b) (now Article 7(1)(b) of the Brussels I Regulation (Recast)) 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

39 The UN Convention 2005, Article 6(2).

40 Ibid.

41 The Brussels I Regulation 2001, Articles 8–14 (governing insurance); Articles 15–17 (governing consumer contracts); and Articles 18–21 (governing employment contracts).

42 The Brussels I Regulation 2001, Article 5(1)(a), states: '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 J. H. C. Morris, D. McClean and K. Beevers (2005) *The Conflict of Laws*, 6th edn (London: Sweet & Maxwell), p. 72.

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[43] can be divided into two categories: one is different obligations have different places of delivery, and the other is the relevant obligation has several places of delivery.

In the first category, there are two possibilities: first, disputes relate to more than one obligation. Article 5(1) (now Article 7(1) of the Brussels I Regulation (Recast)) 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.[44] 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.[45]

In the second category, there are also two possibilities. First, as is noted by the most recent case *Color Drack GmbH* v. *Lexx International Vertriebs GmbH*,[46] there is a query about 'whether the first indent of Article 5(1)(b) of the Brussels I Regulation (now Article 7(1)(b) of the Brussels I Regulation (Recast)) applied in the case of a contract for the sale of goods involving several places of delivery within a single Member State',[47] and if so, 'whether the plaintiff could sue in the court for the place of delivery of its choice'[48] among all places of deliveries. The court ruled that the applicability of the first indent of Article 5(1)(b) (now Article 7(1)(b) of the Brussels I Regulation (Recast)) 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,[49] 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 in which court the plaintiff may sue him, 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 whether the plaintiff can sue in a court of its own choice under Article 5(1)(b) (now Article 7(1)(b) of the Brussels I Regulation (Recast)), 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

43 J. Hill (2005) *International Commercial Disputes in English Courts*, 3rd edn (Oxford and Portland, OR: Hart), p. 135.

44 Case C-420/97 *Leathertex Divisione Sintetici SpA* v. *Bodetex BVBA* [1999] ECR I-6747.

45 Case 266/85 *Shenavai* v. *Kreischer* [1987] ECR 239.

46 *Color Drack GmbH* v. *Lexx International Vertriebs GmbH* (Case C-386/05), [2007] I.L.Pr. 35.

47 [2007] I.L.Pr. 35, p. 456.

48 [2007] I.L.Pr. 35, p. 456.

49 [2007] I.L.Pr. 35, p. 479.

criteria'.[50] If all places of delivery are 'without distinction' and 'have the same degree of closeness to the facts in the dispute',[51] 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) (now Article 7(1)(b) of the Brussels I Regulation (Recast)) 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 (AG)'s opinion, Article 5(1)(b) (now Article 7(1) of the Brussels I Regulation (Recast)) does not apply to this situation as the objective of forseeability of the Brussels I Regulation could not be achieved,[52] that is a single place of performance for the obligation in question could not be identified for the purpose of this provision,[53] then, the claimant should turn to Article 2 of the Brussels I Regulation (now Article 4 of the Brussels I Regulation (Recast)), according to which the court with jurisdiction is that of the domicile of the defendant.

In B2B electronic contracting disputes, can Article 5(1) (now Article 7(1) of the Brussels I Regulation (Recast)) still apply? If so, how can Article 5(1) (now Article 7(1) of the Brussels I Regulation (Recast)) 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 provisions 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 as well as 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).[54] 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

50 *Color Drack GmbH* v. *Lexx International Vertriebs GmbH* (Case C-386/05), [2007] I. L. Pr. 35, p. 480.

51 [2007] I.L.Pr. 35, p. 473.

52 [2007] I.L.Pr. 35, p. 472.

53 Case C-256/00 *Besix SA* v. *Wasserreinigungsbau Alfred Kretzschmar GmbH & Co. KG (Wabag)* [2002] ECR I-1699.

54 J. Fawcett, J. Harris and M. Bridge (2005) *International Sale of Goods in the Conflict of Laws* (New York: Oxford University Press), p. 514.

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.[55]

Secondly, how to distinguish digitised goods 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.[56]

Thirdly, what can be the place of performance of the obligation in question in cyberspace? As discussed before, between businesses the place of delivery is usually included by the contract of sale.[57] 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 good, as there are a number of places where electronic transactions are processed, for example the 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 (now Article 7(1)(b) of the Brussels I Regulation (Recast)), 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 as connecting factors depending on the characteristics of commercial transactions. When selling digitised goods with delivery over the Internet, such as the seller selling the software and the buyer/recipient downloading it onto his computer, the place of performance in question should be the recipient's place of business or domicile, that is the place where the goods are delivered should be regarded as being where the recipient has its place of business or is domiciled. In the author's opinion, in cases of digitised goods with performance over the Internet, the interpretation of 'the place of performance should be regarded as the place where goods were delivered or should

55 R. Burnett and P. Klinger (2005) *Drafting and Negotiating Computer Contracts*, 2nd edn (Haywards Heath: Tottel Publishing), p. 74.

56 J. Fawcett, J. Harris and M. Bridge (2005) *International Sale of Goods in the Conflict of Laws* (New York: Oxford University Press), p. 1301.

57 H. A. Deveci (2006) 'Personal jurisdiction: where cyberspace meets the real world – Part II', *Computer Law and Security Report*, 22: 39–45, at p. 43.

have been delivered' under Article 5(1)(b) of the Brussels I Regulation should be as follows:

> The place of performance should be at a recipient's place of business indicated by the party. If a party has not indicated a place of business, or has more than one place of business, then 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 place of directed online business activities shall be considered to be mostly closely connected with the contract. If there is no place of business, the place of performance shall be at a recipient's domicile.

It is possible that the seller may be resident and have his business in state A, while the actual uploading activities happen in state C and the recipient may download the digitised products when away from his/her residence or principal place of business. In automated computing systems, there is a possibility that a software development contract with several milestones may be transferred individually in different countries to the buyers. Under these circumstances, the principal place of business of the party should be the appropriate *situs* as the place of performance of contract.[58]

In B2C electronic commercial transactions, the Brussels I Regulation (Recast) is also in line with the Brussels I Regulation, providing the determination of jurisdiction 'in matters relating to a contract concluded by a person, the consumer, for a purpose which can be regarded as being outside his trade or profession'.[59] It specifies that 'the contract has been concluded with a person who pursues commercial or professional activities in the Member State of the consumer's domicile or, by any means, directs such activities to that Member State or to several States including that Member State, and the contract falls within the scope of such activities'.[60] This employs the 'pursuing and directing' (equivalent to 'targeting') approach to determine the location for commercial or professional activities. The Brussels I Regime is only applicable if commercial activities have been directed to a Member State of the consumer's domicile or several Member States including the consumer's domicile. Article 15(2) of the Brussels I Regulation (now Article 17(2) of the Brussels I Regulation (Recast)) specifically provides that 'where a consumer enters into a contract with a party who is not domiciled in a Member State but has a branch, agency or other establishment in one of the Member States, that party shall, in disputes arising out of the operations of the branch, agency or

58 F. Wang (2010) *Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US and China* (Cambridge: Cambridge University Press), pp. 56–7.

59 The Brussels I Regulation 2001, Article 15(1); and also the Brussels I Regulation (Recast) 2012, Article 17(1).

60 The Brussels I Regulation 2001, Article 15(1)(c); and also the Brussels I Regulation (Recast) 2012, Article 17(1)(c).

establishment, be deemed to be domiciled in that State'. The general rule of domicile applies to both B2B and B2C contracts, although there are differences in that for B2B contracts defendants (sellers or buyers) domiciled in a Member State shall, whatever their nationality, be sued in the courts of that Member State, whereas, for B2C contracts in cases of proceedings against consumers, jurisdiction shall be determined by the consumer's domicile so that proceedings may only be brought in the courts of the Member State in which the consumer is domiciled.

12.1.2 US jurisdiction tests

Compared with the EU, due to the fact that US companies are at the forefront of Internet technology, litigation regarding e-commerce in the United States 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.[61] 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 exits when the underlying claims arise out of, or are directly related to, a defendant's contacts with the forum state.[62] The US also considers the recipient's place of business as a connecting factor for the determination of specific jurisdiction.

The above notion comes from the famous case *International Shoe Co.* v. *Washington*,[63] which indicated that the minimum contacts test has both a general and a specific component.[64] 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 connection with that state. For example, advertising or having business offices within a state may provide minimum contact 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

61 Hague Convention Status Table. Available at: http://www.hcch.net/index_en.php?act=conventions.status&cid=98 (last accessed 30 June 2013).

62 W. B. Chik (2002) 'U.S. jurisdictional rules of adjudication over business conducted via the Internet – guide-lines and a checklist for the e-commerce merchant', *Tulane Journal of International and Comparative Law*, 10: 243, at pp. 248–9.

63 326 US 310 (1945).

64 E. F. Scoles, P. Hay, P. J. Borchers and S. C. Symeonides (2000) *Conflict of Laws*, 3rd edn (St Paul, MN: West), p. 344.

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.[65] 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.[66] 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.[67] 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.'[68] Thus general jurisdiction results from a party's continuous, systematic and ongoing ties to a certain forum.[69]

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.[70] 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.[71] 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.[72] 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'.[73]

65 *International Shoe*, 326 US at 320, 66 SCt. at 160, 90 LEd. at 104.
66 E. F. Scoles, P. Hay, P. J. Borchers and S. C. Symeonides (2000) *Conflict of Laws*, 3rd edn (St Paul, MN: West), p. 348.
67 Ibid., p. 338.
68 Restatement, Second, Conflict of Laws §30 (1971).
69 *Helicopteros Nacionales de Colombia, S.A.* v. *Hall*, 466 US 408 (1984).
70 E. F. Scoles, P. Hay, P. J. Borchers and S. C. Symeonides (2000) *Conflict of Laws*, 3rd edn (St Paul, MN: West), p. 344.
71 *Ashi Metal Ind. Co.* v. *Superior Court*, 480 US 102 (1987).
72 M. Maloney (1993) 'Specific jurisdiction and the "arise from or relate to" requirement … what does it mean?', *Washington and Lee Law Review*, 50: 1265, at pp. 1269–70.
73 E. F. Scoles, P. Hay, P. J. Borchers and S. C. Symeonides (2000) *Conflict of Laws*, 3rd edn (St Paul, MN: West), p. 300.

In recent 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 contract' sufficient to establish specific personal jurisdiction over a non-resident defendant, at least in the absence of other contacts with the forum state.[74] Whether a defendant can be subject to specific jurisdiction in contract 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.'[75]

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.[76] 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 being 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.[77]

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'.[78] 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 contracts with it such that the maintenance of the suit does not offend traditional notions of fair play and substantial justice.'[79] *Zippo Mfg. Co.* v. *Zippo Dot Com. Inc.*[80] is emerging as the seminal case on whether an Internet website provides the minimum

74 G. J. H. Smith (2002) *Internet Law and Regulation*, 3rd edn (London: Sweet & Maxwell), p. 347.
75 *Burger King Corp.* v. *Rudzewicz*, 471 US 479, 105 SCt. 2185, 85 LEd. 2d 528 (1985).
76 *World Wide Volkswagen* v. *Woodson*, 444 US 286 (1980).
77 *Ballard* v. *Savage*, 65 F.3d 1495, 1498 (9th Cir. 1995).
78 See *Zippo Mfg. Co.* v. *Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W. D. pa 1997), at 1124.
79 *Int'l Shoe Co.* v. *State of Wash.*, 326 US 310 (1945).
80 See *Zippo Mfg. Co.* v. *Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W. D. pa 1997).

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'.[81]

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.[82] 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 website.'[83] 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.[84]

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 in the middle of the scale, one would have expected the court to provide a rough definition of 'interactivity', but it did not.[85] 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 now are 'at least highly interactive, if not integral to the marketing of the website owners'.[86]

81 See *Zippo Mfg. Co.* v. *Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W. D. pa 1997), at 1124.

82 *CompuServe Inc.* v. *Patterson*, 89 F. 3d. 1267 (6th Cir. 1996).

83 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).

84 See *Zippo Mfg. Co.* v. *Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W. D. pa 1997), at 1124.

85 B. D. Boone (2006) 'Bullseye! Why a "targeting" approach to personal jurisdiction in the e-commerce context makes sense internationally', *Emory International Law Review*, 20: 241, at p. 258.

86 D. T. Rice (2004) 'Problems in running a global Internet business: complying with the laws of other countries', *PLI/PAT*, 797: 11, at p. 52.

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*.[87] 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.[88] 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,[89] because determining where a larger, multi-forum corporation is 'harmed' is a difficult prospect.[90] 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.'[91]

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'.[92] 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'.[93] 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 test, places greater emphasis on identifying the intentions of the parties and the steps taken to either enter or avoid a particular jurisdiction.[94] Further, the advocates of the targeting test view it as a better and fairer approach for determining whether the defendant reasonably anticipated being haled into a foreign court to answer for their activities in the foreign

87 *Calder* v. *Jones*, 465 US 783 (1984). In *Calder*, a California resident brought suit in the 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.'

88 B. D. Boone (2006) 'Bullseye! Why a "targeting" approach to personal jurisdiction in the e-commerce context makes sense internationally', *Emory International Law Review*, 20: 241, at p. 260.

89 Ibid., p. 261.

90 D. T. Rice and J. Gladstone (2003) 'An assessment of the effects test in determining personal jurisdiction in cyberspace', *Business Law*, 58: 601, at p. 629.

91 *Cybersell, Inc.* v. *Cybersell, Inc.*, 130 F. 3d 414, 420 (9th Cir. 1997).

92 *Bancroft & Masters, Inc.* v. *Augusta Nat'l Inc.*, 223 F. 3d 1082, 1087 (9th Cir. 2000).

93 223 F. 3d 1082, 1087 (9th Cir. 2000)

94 M. Geist (2001) 'Is there a there there? Toward greater certainty for Internet jurisdiction', 661 *PLI/PAT*, 661: 561, at p. 575, and (2001) *Berkeley Technology Law Journal*, 16: 1345, at p. 1362.

forum state.[95] This determination is central to the due process analysis articulated by the United States 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 haled 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'.[96]

The measures of the 'targeting approach' in international contracts of sale are threefold. First, it is based on the intentions of the defendant: the defendant must 'direct' electronic activity into the forum state[97] and show a 'deliberate or intended action' in order to generate consistent results.[98] Second, the defendant must intend to engage in business or other interactions ('something more') in the forum state. Third, 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. According to the above rules, the recipient's place of business or domicile is most likely to be tackled for purposefully and deliberately directing and targeting sale of goods and provision of services. Thus the determination of the targeting approach in the US has some similarities to that of the place of performance of the obligation in the EU regarding the sale of goods over the Internet.

12.1.3 Chinese legislation relating to Internet jurisdiction

There is no particularised Internet jurisdiction legislation promulgated in China. Jurisdictional issues are referred to the general international or national procedural rules covering jurisdiction. Chapter II of the Civil Procedure Law of the People's Republic of China[99] 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), although the Civil Procedure Law does not provide specific jurisdiction provisions. There are four categories of jurisdiction in the Chinese People's Courts: tier jurisdiction (subject to the level of cases),

95 M. Geist (2001) 'Is there a there there? Toward greater certainty for Internet jurisdiction', *PLI/PAT*, 661: 561, at p. 575, and (2001) *Berkeley Technology Law Journal*, 16: 1345, at p. 1362.

96 *World-Wide Volkswagen Corp.* v. *Woodson*, 444 US 286, 297 (1980).

97 C. Aciman and D. Vo-Verde (2002) 'Refining the Zippo test: new trends on personal jurisdiction for Internet activities', *Computer and Internet Law*, 19: 16, and also *ALS Scan, Inc.* v. *Digital Serv. Consultants, Inc.*, 293 F. 3d 707, 714 (4th Cir. 2002).

98 B. D. Boone (2006) 'Bullseye! Why a "targeting" approach to personal jurisdiction in the e-commerce context makes sense internationally', *Emory International Law Review*, 20: 241, p. 266.

99 Articles 237–270, Civil Procedure Law of the People's Republic of China, promulgated on 9 April 1991.

territorial jurisdiction (subject to the connecting factors), transferred jurisdiction (subject to the competency of the courts first seised) and designated jurisdiction (intertwined with transferred jurisdiction). In terms of jurisdictional rules there are three underlying doctrines: exclusive clauses/agreements, general jurisdiction and special jurisdiction.

Exclusive jurisdiction clauses/agreements

The principle of 'party autonomy' is generally recognised by the Civil Procedure Law in China, which enables parties to negotiate their jurisdiction agreement. Article 34 (originally Article 25) of the China Civil Procedure Law 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.'[100]

On 31 August 2012 the Decision of the Standing Committee of the National People's Congress on Amending the Civil Procedure Law of the People's Republic of China (2012) was adopted by the Standing Committee of the National People's Congress. Article 25 of the Civil Procedure Law was amended to become Article 34 providing that:

> The parties to a contractual dispute or *any other property dispute* may choose through agreement stipulated in the written contract that the people's court in the place which have arisen or which may arise *in actual connection with* a particular legal relationship or dispute shall have jurisdiction, such as 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 subject matter is located, provided that the provisions of this Law regarding jurisdiction by level and exclusive jurisdiction shall not be violated.[101] (Emphasis added)

The new provision expands the scope of jurisdictional agreements and specifies the requirement of an actual connection factor with a dispute for a chosen court, though the five sample connecting factors remain the same.

With the promulgation of the China and Hong Kong Arrangement in 2008, an exclusive choice of court agreement for commercial contracts in

100 The Civil Procedure Law of the People's Republic of China (as amended by the Decision of August 31, 2012 on Amending the Civil Procedure Law of the People's Republic of China), which came into force on 1 January 2013, Article 34 (originally Article 25).

101 Decision of the Standing Committee of the National People's Congress on Amending the Civil Procedure Law of the People's Republic of China, adopted on 31 August 2012 and effective on 1 January 2013, Order No. 59 of the President of the People's Republic of China.

relation to the money judgments is also explicitly recognised. It will, therefore, enhance the enforcement of the jurisdiction agreement when the exclusive chosen court of Hong Kong or China in the agreement is valid and such agreement is formed after the China and Hong Kong Arrangement has come into effect.[102] With regard to the arrangement between the Mainland and Macao, there is no indication and provision of the recognition of exclusive choice of court agreements under the Arrangement between the Mainland and Macao Special Administrative Region on the Mutual Recognition and Enforcement of Civil and Commercial Judgments in 2006.[103]

Although the Civil Procedure Law does not have a precise explanation of conditions of the validity and enforceability of the jurisdiction agreement, it is clear that the jurisdiction agreement shall be in writing. In the information society, jurisdiction agreements concluded by electronic means should be equivalent to agreements in writing as Chinese national laws or arrangements interpret 'in writing' as 'including electronic means'. For example, the China Contract Law in 1999[104] implements several changes in contract formation rules. For example, a contract can now be made in any manner.[105] Under the China Contract Law, writings include agreements, letters, telegrams, telexes, faxes, electronic data information and electronic mail.[106] Article 2 of the China Electronic Signatures Law in 2005 recognises the validity of electronic signatures to contracts.[107] Article 3 of the Arrangement between the Mainland and the Hong Kong Special Administrative Region on Reciprocal Recognition and Enforcement of the Decisions of Civil and Commercial Cases under Consensual Jurisdiction in 2008 (hereafter 'the China and Hong Kong Arrangement') also provides that agreements can be concluded by electronic means including telegraph, fax, electronic data exchange and e-mail. It allows an exclusive choice of court agreement by one single document or several documents. It further clarifies that an exclusive choice of court agreement is an independent agreement to the relevant contracts. Thus the amendment,

102 Arrangement on Mutual Recognition and Enforcement of Judgments in Civil and Commercial Matters by Courts of Mainland and Hong Kong SAR Pursuant to Agreed Jurisdiction by Parties Concerned, Fa Shi No. 9 [2008]. Available at: http://sg2.mofcom.gov.cn/aarticle/chinalaw/foreigntrade/200807/20080705695854.html (last accessed 30 June 2013).

103 Arrangement Between the Mainland and the Macao Special Administrative Region on the Mutual Recognition and Enforcement of Civil and Commercial Judgments, Signed at Macau SAR, on 28 February 2006, Fa Shi No. 2 [2006]. Available at: http://en.io.gov.mo/Legis/International/record/612.aspx (last accessed 30 June 2013).

104 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.

105 The China Contract Law 1999, Article 10, states: 'A contract may be made in a writing, in an oral conversation, as well as in any other form.'

106 The China Contract Law 1999, Article 11.

107 Law of the People's Republic of China on Electronic Signature, 28 August 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.wipo.int/wipolex/en/text.jsp?file_id=182409 (last accessed 30 June 2013).

revocation or termination of the contracts will not affect the validity of the exclusive choice of court agreement, except as otherwise agreed in a written agreement signed by both. In practice, jurisdiction clauses or agreements were not strictly recognised and enforced. For example, in the case of *Zhejiang Province Arts & Crafts Import & Export Industrial and Trade Group* v. *HongKong Golden Fortune Shipping Co. Ltd*, although there was a choice of court agreement in the bill of lading that 'any disputes in relation to the bill of lading shall be handled by Hong Kong courts in accordance with Hong Kong law', it was not recognised and enforced by the Shanghai Maritime Court that first seised the case for the reason of *forum non conveniens*.[108] In the case of *Nedco International Inc* v. *NingBo Yinzhou Ledeshi Light-made Factory and Ningbo Ledeshi Electronic Equipment Co. Ltd*, there was a jurisdictional clause in their international contract for the provision of exclusive services stating that 'California courts have jurisdiction and Californian laws shall apply'. Nedco first sued Deleshi for supplying unqualified light bulbs which were not fit for purpose of sale in the US market in Ningbo Intermediate People's Court. The Supreme People's Court of Zhejiang Province upheld the decision of Ningbo Intermediate People's Court that Chinese law shall apply as Chinese law had the closest relation to this dispute in that both defendants were domiciled in China. The Supreme Court also affirmed that Nedco could only return goods that did not meet the criteria but had no right to return goods that did meet the criteria.[109] The determination of jurisdiction in this case is in line with Article 244 of the Civil Procedure Law which applies to international cases, requiring that parties should choose the court which has substantial connection with the dispute. Subsequently there may be concern over the relationship between the principles of 'party autonomy' and 'closest relation' and their deployment, which require judicial interpretation and further clarification.

General jurisdiction

In general Article 24 of the Civil Procedure Law employs the 'domicile' rule 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'.[110] There are three core interpretations of the Civil Procedure Law issued by the Supreme Court to help implement jurisdiction issues: the 1992 Opinions of the Supreme Court on the Implementation of the Civil Procedure Law; the 1998 Regulations of the

108 *Zhejiang Province Arts & Crafts Import & Export Industrial and Trade Group* v. *HongKong Golden Fortune Shipping Co. Ltd*, September 1988, Supreme People's Court, Selected Cases of People's Courts (1996) 1711–17 (Shanghai Maritime Court 1991).

109 *Nedco International Inc.* v. *NingBo Yinzhou Ledeshi Light-made Factory and Ningbo Ledeshi Electronic Equipment Co. Ltd.*, the People's Supreme Court in Zhejiang Province, (2005) Zhe Ming San Zhong Zi, No. 287.

110 The China Civil Procedure Law (amended in 2012), Article 24.

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.

Special jurisdiction

In addition to the principle of the 'closest relation' and 'practical connections' provided in Article 244, with regard to disputes concerning foreign joint ventures, Article 246 of the Civil Procedure Law specifies 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'.

Furthermore, Article 243 of the Civil Procedure Law 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. For example, the case of *Marubeni America Corporation* v. *Weihai Shan Hai Guang Xing Leather Co. Ltd and Wei Hai Jinfreng Transportation Agent* concerned the acceptance of delivery of goods without the original bills of lading. The Qingdao Maritime Court confirmed that it had jurisdiction over the actions in question because the port of destination was Weihai Habour in Shandong Province.[111] It is advised that if there is a conflict between the actual place of performance of the contract and the designated place of performance of the contract, the designated place of performance of the contract should be deemed as the connecting factor for determining jurisdiction. Consequently the courts located in the designated place of performance of the contract have jurisdiction.[112] For example, in the case of *Dongdianhua Investment Co. Ltd (Shanghai)* v. *CCID Consulting Company Ltd (Beijing)*, Dongdianhua claimed that the actual place of performance of the contract had changed from Beijing (the place of performance agreed in the contract) to Shanghai as CCID submitted the performance report to Dongdianhua by e-mail which was executed in Shanghai after review.[113] The Court of Second Instance affirmed that the

111 *Marubeni America Corporation* v. *Weihai Shan Hai Guang Xing Leather Co. Ltd and Wei Hai Jinfreng Transportation Agent*, Qingdao Maritime Court, Qinghai Fa Hai Shang Chu Zi. No. 126 [2009].

112 Supreme People's Court on the Reply to the Special Arrangement of the Place of Performance for the Contract of Sales, 19 August 1990, Fa (Jing) Fu No. 11 [1990].

113 *Dongdianhua Investment Co. Ltd (Shanghai)* v. *CCID Consulting Company Ltd.(Beijing)*, Beijing Haidian District People's Court. Yi Zhong Min Zhong Zi No. 10261 [2007].

Court of First Instance, Beijing Haidian District People's Court, had jurisdiction as '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' according to Article 24 of the Civil Law Procedure Law. Moreover, the contract explicitly indicated that the place of the performance of the contract was Beijing Haidian District.

In contrast, in the case of *Avnet Technology (Hong Kong) Ltd* v. *JiaTong Technology (Suzhou) Ltd* (2009) in a dispute over a contract for the sale of goods, the Civil Division of the Intermediate People's Court of Suzhou recognised it as a foreign-related lawsuit where the foreign jurisdiction section of the Civil Procedure Law of China shall be applied as the plaintiff was a habitual resident in Hong Kong and therefore outside of the jurisdiction of mainland China.[114] The Intermediate People's Court of Suzhou had jurisdiction over the dispute as the defendant – JiaTong Technology (Suzhou) Ltd – was located in Suzhou. It is notable that the Intermediate People's Court of Suzhou also accepted the evidence of four purchase orders and two e-mail messages submitted by the plaintiff, Avnet Technology Hong Kong Ltd. Thus, in practice, e-mail messages can be served as evidence in the courts of China.

Sometimes, the court of the place in which the contract is performed or carried out will also exercise jurisdiction. For example, in the case of *Chamber of Japan in Shanghai* v. *Huida Co. (Hong Kong)* regarding a dispute over an investment agreement, neither of the parties had offices in mainland China, but the Intermediate People's Court of Ningbo exercised jurisdiction over the case as the contract was performed in Ningbo city in Zhejiang Province.[115]

In the author's opinion, the jurisdiction provision in the Civil Procedure Law needs more clarification when referring to international contracts for the sale of goods. With emerging Internet-related contractual disputes, the Civil Procedure Law may appear to be increasingly insufficient. There is also a lack of jurisdictional provisions in the China Electronic Signatures Law. Relevant measures have been proposed and adopted to fill the gaps including the Management of Chinese Computer Information Networks connected to International Networks Regulation[116] and the Computer Information Network and Internet Security, Protection and Management Regulation.[117] These two

114 *Avnet Technology (Hong Kong) Ltd* v. *JiaTong Technology (Suzhou) Ltd*, the Intermediate People's Court of Suzhou, No.0027 [2009].

115 *Chamber of Japan in Shanghai* v. *Huida Co. (Hong Kong)* (1994) the Intermediate People's Court of Ningbo, from Selected Cases of the Higher People's Court of Zhejiang Province, 1994.

116 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 accessed 30 June 2013).

117 Computer Information Network and Internet Security, Protection and Management Regulations. Available at: http://www.woodmedia.com/cinfolink/netregs.htm (last accessed 30 June 2013).

regulations cover both civil and criminal issues. However, the rules relating to jurisdiction are still largely insufficient.

Overall, according to Chinese law, there are six basic principles to determine the jurisdiction: the domicile principle,[118] the personal jurisdiction principle,[119] the freedom of choice principle (party autonomy),[120] the principle of related location[121] and the territorial jurisdiction principle (known as 'the exclusive jurisdiction principle').[122] The fundamental jurisdiction rule in a 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 has habitual residence. With regard to disputes concerning B2B foreign-related contracts of sale, the court in the place where the contract was performed shall have jurisdiction unless parties otherwise agree on exclusive jurisdiction.

Summary: a comparative study

The EU and US both signed the Hague Convention on Choice of Court Agreements in 2009, which is considered to be an important step in improving the harmonisation of private international law. The EU special jurisdiction approach and the US specific jurisdiction approach are different in that the Brussels I Regulation in the EU provides comprehensive rules on judicial cooperation between member states, while the US adopts a market-oriented jurisdiction approach. For example, the US employs 'Zippo', 'effects' and 'targeting' tests to determine Internet jurisdiction, while 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

118 According to the related law, whatever their nationality, a lawsuit will be sued in the court 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. The China Civil Procedure Law (amended in 2012), Article 26.

119 That is, nationality principle. The China Civil Procedure Law (amended in 2012), Article 22.

120 The China Civil Procedure Law (amended in 2012), Article 25.

121 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.

122 The China Civil Procedure Law (amended in 2012), Articles 22–35 (exclusive jurisdiction in Article 34); and also Articles 243–246 (cases involving foreign elements).

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 (now Article 7(1)(b) of the Brussels I Regulation (Recast)), 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) of the Brussels I Regulation (now Article 7(1) of the Brussels I Regulation (Recast)).[123] In the author's view, the fundamental principle or philosophy of Article 7(1) of the Brussels I Regulation (Recast) will not be diminished by introducing an additional clause to further interpret 'the place of performance' in cyberspace. This, on the contrary, should enhance the consistency of the implementation of the determination of 'the place of performance' and 'the place of delivery' taking into account special connecting factors in Internet-related disputes. Amending or revising the current legislation is feasible. However, it would still take enormous time to draft a specific regulation or convention and for it to come into force. This would certainly be against the pace of technological developments and their immediate impacts. It is conceivable that in the near future the new fast-developing electronic communications may well prove that existing laws and judicial interpretations are no longer suitable or applicable to new concepts due to different connecting factors. A special regime of jurisdictional rules for electronic commerce would then be introduced on the ground that traditional territorially based concepts of jurisdiction were no longer entirely appropriate to regulate cyberspace.

Compared with the EU and US, China has a very similar approach, which comprises the principle of 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. There is a need to have a single national law specifying jurisdictional issues, in particular concerning foreign Internet disputes, which may increase foreigners' confidence in doing business in China.

12.2 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

123 J. Fawcett, J. Harris and M. Bridge (2005) *International Sale of Goods in the Conflict of Laws* (New York: Oxford University Press), p. 594.

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 law applicable to online commercial transactions as opposed to offline commercial transactions the difference only arises when transactions involve digitised goods with electronic delivery.

12.2.1 The EU approach

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',[124] which relates to 'online activities', such as 'online information, online advertising, online shopping, and online contracting'.[125] 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.[126]

One of the most important instruments regulating applicable law in the EU is the Rome Convention of 1980 (the Rome Convention).[127] 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

124 EC Directive on Electronic Commerce 2000, Article 3(1).

125 EC Directive on Electronic Commerce 2000, Recital 21.

126 J. Fawcett, J. Harris and M. Bridge (2005) *International Sale of Goods in the Conflict of Laws* (New York: Oxford University Press), p. 1233.

127 Convention on the Law Applicable to Contractual Obligations (the Rome Convention 1980), latest consolidated version, 30 December 2005, OJ C334/1.

applies 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 to make 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)[128] 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.'[129]

On 17 June 2008 the Regulation of the European Parliament and the Council on the law applicable to contractual obligations (Rome I) was adopted by the European Parliament and the Council.[130] 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.[131] Rome I shall apply to contracts concluded after 17 December 2009.[132]

The Rome I Regulation is intended 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[133] (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 with normal contracts, contracts made via electronic communications may also insert a choice of law agreement/clause. In absence of a choice of law clause, it will be even more difficult to determine applicable law than normal contracts due to the unique features of electronic communications.

128 Proposal for a Regulation of the European Parliament and the Council on the Law Applicable to Contractual Obligations (Rome I), Brussels, 15 December 2005, COM (2005) 650 final 2005/0261 (COD).

129 '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.

130 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 L177/6-16, 4 July 2008.

131 The Rome I Regulation 2008, Article 24(1).

132 The Rome I Regulation 2008, Article 28.

133 OJ L12, 16 January 2001, p. 1.

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[134] 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 has 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 replaces Article 3(3) of the Rome Convention, providing more comprehensive rules on parties' freedom of choice of law. Article 3(3) and (4) emphasises that the chosen law should govern the case 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) of the Rome I Regulation 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 to subject the different obligations to different laws. This is known as 'splitting the applicable law'.[135] This may be divided up 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;[136] thirdly, different groups of obligations may be governed by different laws;[137] fourthly, the obligations of each party may be governed by a different law.[138]

Moreover, parties must have freedom to re-choose their chosen law. Article 3(2) of the Rome I Regulation 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

134 M. Wilderspin (2008) 'The Rome I Regulation: communitarisation and modernisation of the Rome Convention', *ERA Forum*, 9: 259–74 (ERA: Academy of European Law).

135 J. Hill (2005) *International Commercial Disputes in English Courts*, 3rd edn (Oxford and Portland, OR: Hart), p. 481.

136 Giuliona – Lagarde Report, [1980] OJ C282/1, p. 17.

137 O. Lando (1987) 'The EEC convention on the law applicable to contractual obligations', *Common Market Law Review*, 24: 159–214, at p. 168.

138 C. McLachlan (1990) 'Splitting the proper law in private international law', *British Yearbook of International Law*, 61: 311.

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.[139]

With regard to requirements as to form, however, neither the Proposal for Rome I Regulation (in the review process) nor the Rome I Regulation set out a provision expressly affirming the 'function equivalent' rule for electronic mail. The International Chamber of Commerce (ICC) and the United Kingdom government responded to the Green Paper on the conversion of the Rome Convention into a Community instrument[140] (hereafter 'Green Paper') on whether Article 9 of the Rome Convention[141] should be reformed. According to the opinion of the ICC and the UK, Article 9 of the Rome Convention adequately covered contracts concluded by e-mail, thus there should be no need to modify this article[142] because a contract concluded by e-mail 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 e-mail, 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.

139 J. Hill (2005) *International Commercial Disputes in English Courts*, 3rd edn (Oxford and Portland, OR: Hart), p. 482.

140 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 January 2003, Commission of the European Communities. Available at: http://eur-lex.europa.eu/LexUriServ/site/en/com/2002/com2002_0654en01.pdf (last accessed 30 June 2013).

141 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*.

142 Document 373-33/8, p.6; Response of the Government of the United Kingdom. Available at: http://ec.europa.eu/justice_home/news/consulting_public/rome_i/doc/united_kingdom_en.pdf (last accessed 30 June 2013), p. 8.

> This solution has made it unnecessary to take a more or less artificial decision on the location of a contract between distant parties.[143]

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 (hereafter 'the UN Convention'), the place of dispatch or receipt of an electronic communication is the place where the party has its place of business,[144] but if the party does not have a place of business, reference should be made to his habitual residence.[145] 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 the 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.[146]

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),[147] adding 'habitual residence' as a linking factor. Article 10 of the proposal is subsequently adopted in Article 11 of the Rome I Regulation, which is more accurate but without substantially changing the content. The provision of 'the formal validity' (Article 11 of the Rome I Regulation) 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

143 Green Paper, p. 39, COM (2002) 654 final, Brussels, 14 January 2003.
144 The UN Convention 2005, Article 10(3).
145 The UN Convention 2005, Article 6(3).
146 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 January 2003).
147 The Rome I Regulation 2008, Article 11.

> 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.[148]

It is obvious that the provision of the formal validity does not explicitly recognise the 'functional equivalence' principle as to a choice-of-law clause/agreement concluded by electronic means, although the Rome I Regulation (Recital 40) clarifies that:

> the application of provisions of the applicable law designated by the rules of this Regulation should not restrict the free movement of goods and services as regulated by Community instruments, such as 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).[149]

In addition, the Rome I Regulation impliedly recognises the 'electronic means' by addressing 'by any means' in its Recital 25, which provides that 'the same protection should be guaranteed if the professional, while not pursuing his commercial or professional activities in the country where the consumer has his habitual residence, directs his activities *by any means* to that country or to several countries, including that country, and the contract is concluded as a result of such activities.'[150]

In the author's opinion, the recognition of the exclusive jurisdiction agreements concluded by electronic means under the Choice of Court Convention should also be applicable to the recognition of the choice of law agreements concluded by electronic means. For example, a subsidiary rule concerning the validity of electronic communications can 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 as follows:

> 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.[151]

148 Proposal for a Regulation of the European Parliament and of the Council on the law applicable to contractual obligation (Rome I), Council of the European Union, 13853/06, LIMITE, JUSTCIV 224, CODEC 1085, Brussels, 12 October 2006, Articles 10(1) and (2).

149 The Rome I Regulation 2008, Recital 40.

150 The Rome I Regulation 2008, Recital 25.

151 Employed from Article 3(c) of the Choice of Court Convention.

References concerning the choice of law rules concluded by electronic means can also be found in 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. It is notable that 'party autonomy' is the core principle of the UN Convention. This freedom also extends to the amendment of choice of law clauses after the formation of contracts. The revised choice of law clause that parties newly agree will not affect the validity of the existing contract. The provision of 'error in electronic communications'[152] in the UN Convention also supports the above principle. It provides that the information system should provide the other party with an opportunity to correct the input error. Accordingly parties might have an opportunity to add or amend a choice of law clause in the 'additional information' or 'comments' space box on a website. Parties might also enclose or upload a document expressing the intention to change the applicable law when communicating an acceptance to the offeror by electronic means. Alternatively parties might put forward another e-mail followed by their transaction noting the amendment of the applicable law. It may resort to the rules of the battle of the 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.[153] 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 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'.[154] For a contract of sale or the provision of services, the Rome I Regulation (Article 4) has preserved the rule in the

152 The UN Convention 2005, Article 14.

153 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 'the Green Paper'), COM (2002) 654 final, Brussels, 14 January 2003, Commission of the European Communities, p. 25. Available at: http://eur-lex.europa.eu/LexUriServ/site/en/com/2002/com2002_0654en01.pdf (last accessed 30 June 2013).

154 Proposal for the Rome I Regulation, p. 5.

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.[155] It provides that:

(a) a contract of sale shall be governed by the law of the country in which the seller has his habitual residence;[156] and
(b) a contract for the provision of services shall be governed by the law of the country where the service provider has his habitual residence.[157]

Following Article 4(1) of the Rome I Regulation, it then provides additional rules in Article 4(2) to (4) of the Rome I Regulation as follows:

(2) Where the contract is not covered by paragraph 1 or where the elements of the contract would be covered by more than one of points (a) to (h) of paragraph 1 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.
(3) Where it is clear from all the circumstances of the case that the contract is manifestly more closely connected with a country other than that indicated in paragraphs 1 or 2, the law of that other country shall apply.
(4) Where the law applicable cannot be determined pursuant to paragraphs 1 or 2, the contract shall be governed by the law of the country with which it is most closely connected.[158]

It is clear that the doctrine of the seller's or service provider's 'habitual residence' is the primary rule for the determination of special jurisdiction for the contract of sale or provision of service. Where characteristic performance of the contract cannot be identified, the benchmark of the law of the country with which it is 'manifestly more closely connected' or 'most closely connects' should apply to determine the applicable law. That is, 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 in the application of Article 4, the Rome I Regulation 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 place of business

155 The Rome I Regulation 2008, Article 4(1).
156 The Rome I Regulation 2008, Article 4(1)(a).
157 The Rome I Regulation 2008, Article 4(1)(b).
158 The Rome I Regulation 2008, Article 4(2)–(4).

shall be considered to be the habitual residence of a natural person acting in the course of his business activity; and the place of central administration should be considered as the habitual residence of companies. 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', while Article 4(2) of the Rome Convention would determine it as the principal place of business.

With regard to applicable law in electronic contracts, to determine the applicable law in the absence of choice is a two-stage exercise. The first stage is to ascertain the seller's habitual residence. 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',[159] which is different from the Rome Convention which starts with the 'close connection' principle first. Secondly, if the seller's habitual residence cannot be determined, the court will identify the characteristic performance of the contract and determine the law which is most closely connected to the contract.

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.' The Rome I Regulation (Recital 24) also clarifies that the declaration also states that:

> the mere fact that an Internet site is accessible is not sufficient for Article 15 to be applicable, although a factor will be that this Internet site solicits the conclusion of distance contracts and that a contract has actually been concluded at a distance, by whatever means. In this respect, the language or currency which a website uses does not constitute a relevant factor.[160]

Overall, the Rome I Regulation is more precise for parties to determine the applicable law in both B2B and B2C commercial matters in that the principle of 'habitual residence' has been set as a primary rule. The clearer layers for special jurisdiction may also make it more adaptable to the application of choice-of-law rules for Internet-related B2B contracts of sale or services by firstly finding the seller's or service provider's habitual residence and then determining the place that 'effects the characteristic performance of the contract' and is closely connected with the contract where more appropriate.

159 The Rome I Regulation 2008, Article 4(1)(a).
160 The Rome I Regulation 2008, Recital 24.

12.2.2 The US approach

Unlike the EU, the US has a special provision governing choice of law in the Uniform Computer Transactions Act (UCITA). Although the UCITA only applies to computer information transactions such as computer software, online databases, software access contracts or e-books[161] involving licensing contracts, the model 'choice of law' provision in UCITA can be learned or adopted to the determination of the applicable law in general electronic contracting for the reason that the feature of online contracts involved with digitised delivery will be identical to that of computer information transactions. Without a uniform piece of 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 the law applicable to contracts concluded and performed electronically.

Similar to the EU, there are two core doctrines in ascertaining applicable law: freedom of choice and in the 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.[162] Party autonomy is recognised by Section 109(a) of the Uniform Computer Information Transactions Act (UCITA), by Section 187 of the Second Restatement as well as by Section 1–105 of the Uniform Commercial Code.[163] In the absence of parties' choice, Section 109 of UCITA and Section 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, the UCC (Section 1–105) 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 (Section 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 (Section 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

161 UCITA, Section 103.

162 E. F. Scoles, P. Hay, P. J. Borchers and S. C. Symeonides (2000) *Conflict of Laws*, 3rd edn (St Paul, MN: West), p. 858.

163 Ibid., p. 861.

of a state'.[164] The UCITA expressly deals with choice of law issues. Section 109(a) of the UCITA states that 'parties in their agreement may choose the applicable law', but such choices are not enforced if they are determined to be unconscionable.[165] Under the UCITA (Section 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 respects. 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, while traditionally the EU does not require the chosen law to have any real connection with the parties or the subject matter of their contract,[166] although the new legislation – the Rome I Regulation – has promoted the principle of 'habitual residence' or 'most closely connected' factors. Secondly, in the US, the Second Restatement invalidates the choice of law clause 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, while in the EU, the Rome Regime only prevents the parties to opt out of the mandatory rule. To illustrate the 'mandatory rules' of the Rome Regime, 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. It is arguable that the adoption of party autonomy in the US is intertwined so closely with the far-reaching analysis of interests and policies which, to a great extent, lead to the restriction on its implementation.[167]

The basic methodology in the choice of law is to characterise the issue or question to fit into a category, to determine the connecting factor for that

164 The Second Restatement, Section 187(2) states: 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.

165 F. G. Mazzotta (2001) 'A guide to e-commerce: some legal issues posed by e-commerce for American businesses engaged in domestic and international transactions', *Suffolk Transnational Law Review*, 24: 249, at p. 252.

166 *Vita Food Products Inc.* v. *Unus Shipping Co. Ltd* [1939] AC 277.

167 M. Zhang (2006) 'Party autonomy and beyond: an international perspective of contractual choice of law', *Emory International Law Review*, 10: 511–62, at p. 515.

category and then to apply the law indicated by that connecting factor.[168] 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).[169] 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 e-mail, is 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,[170] that is, the buyer can reassess 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. Having once clicked the 'I agree' button, the parties will be deemed to consent to the terms and conditions, although parties still have a chance of correcting the error in electronic communications as soon as possible after having learned of the error. Subsequently a battle of forms may be likely to occur. This again will resort to the discussion in Part II of this book.

The applicable law in the absence of choice

Section 1–105 of the UCC provides that in the absence of a choice of law agreement 'this Act applies to transactions bearing an appropriate relation to this state'. Under the Second Restatement (Section 188), where a choice of law provision is absent from a contract, the court has to determine whether

168 T. M. Yeo (2004) *Choice of Law for Equitable Doctrines* (New York: Oxford University Press), p. 1.

169 D. T. Rice (2000) 'Jurisdiction in cyberspace: which law and forum apply to securities transactions on the Internet?', *University of Pennsylvania Journal of International Economic Law*, 21: 585, at p. 608.

170 The UN Convention 2005, Article 9(4).

to apply the substantive laws of one state over another in resolving the issues presented before it. Section 188(1) of the Second Restatement determines the applicable law in the 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 the Second Restatement (Section 6).[171] Section 188(2) of the Second Restatement 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 the Second Restatement (Section 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.[172]

Furthermore, both the Second Restatement (Section 191) and the UCC (Sections 1–105(1) and 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, Section 1–105(1) provides for the application of forum law whenever the transaction bears an 'appropriate relation' to the forum.[173]

However, while the Second Restatement (Section 188) governs contracts of sale for both goods and services, Section 191 specifically regulates the sale

171 Section 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.

172 Except as otherwise provided in § 189–199 and 203, provided by § 188(3) of the Second Restatement.

173 E. F. Scoles, P. Hay, P. J. Borchers and S. C. Symeonides (2000) *Conflict of Laws*, 3rd edn (St Paul, MN: West), p. 898.

of goods. The Second Restatement (Section 204) also provides, for all contracts, that a contract should be construed under the law generally applicable under Section 188 of the Second Restatement (the place of the most significant relationship). Furthermore, the Second Restatement (Section 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 Section 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',[174] or the law of the place of making,[175] as the two often coincide on the facts of a given case.[176]

With regard to digitised goods and services, Section 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 Section 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.[177] In the author's view, the action and nature of a licensor who transfers computer information and electronically deliveries a copy of software containing information, is identical to that of a seller concluding a contact 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 has his habitual residence or main place of business should govern the applicable law.

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

174 *Sander* v. *Doe*, 831 F.Supp.886 (S.D.Ga.1993).

175 *International Harvester Credit Corp.* v. *Risks.*, 16 N.C. App. 491, 192 S.E. 2d 707 (1972).

176 *McLouth Steel Corp.* v. *Jewell Coal & Coke Co.* 570 F. 2d 594, 601 (6th Cir. 1978), cert. dismissed 439 US 801, 99 S.Ct. 43, 58 L.Ed.2d 94 (1978).

177 § 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.'

similar protections and rights to a party located in a domestic jurisdiction.[178] Section 109(d) of the UCITA 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.[179]

That is, under the UCITA the doctrine of 'habitual residence' is not considered a primary rule but one of the connecting factors to determine 'the most significant relationship to the transaction'.

Among all possible connecting factors, it appears that the 'place of contracting' may 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', suppose for instance that seller A sold software to buyer A 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 sale 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 which 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 the UCITA. According to the findings regarding the law applicable in B2B electronic contracts, the place which has the most

178 UCITA, Section 109(c).

179 UCITA with prefatory note and comments. Available at: http://www.law.upenn.edu/bll/ulc/ucita/2002final.htm (last accessed 30 June 2013).

significant relationship to the contract or transaction is mostly likely to be the seller's place of business. For B2B electronic contracts, the primary rule is that the law of the seller's place of business should be considered the law of the country that has the closest relationship to electronic contracts or transactions, which is compatible with the primary rule in the Rome I Regulation that the law of the country in which is located the seller's or service provider's habitual residence should first be sought to determine the appropriateness of its application. The common ground lies in the referral to the seller's place.

12.2.3 The Chinese approach

In China, the two general principles of determining applicable law for the contract of sale are the same as those in the EU and US: first is the principle of 'party autonomy', that parties are free to choose the applicable law governing the contract; and 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 the absence of choice. However, China is a civil law country with written laws. There would be no domestic choice of law in contractual matters in China unless the contract included an 'international' element.[180] 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 is located outside of China), or (c) the conclusion or performance of the contract is made in a third country.[181] In December 2012 the Supreme People's Court adopted the Interpretation on Several Issues Concerning the Application of the PRC Law on the Application of Laws to Foreign-related Civil Relationships (1) (hereafter 'the Interpretation') which came into force on 7 January 2013.[182] The Interpretation (Article 1) clarifies five criteria for the determination of a foreign-related civil relationship as follows:

1. One of the parties or both parties are foreign citizens, foreign legal persons or other organisations or stateless persons.
2. One of the parties or both parties have their habitual residence outside the territory of the People's Republic of China.
3. The subject matter is situated outside the territory of the People's Republic of China.

180 M. Zhang (2006) 'Choice of law in contracts: a Chinese approach', *Northwestern Journal of International Law and Business*, 26: 289, at p. 297.

181 M. Zhang (2006) 'Choice of law in contracts: a Chinese approach', *Northwestern Journal of International Law and Business*, 26: 289, at p. 298; see also Article 178 of Organic Law of the People's Courts, promulgated by the National People's Congress in 1979.

182 Interpretation on Several Issues Concerning the Application of the PRC Law on the Application of laws to Foreign-related Civil Relationships (1), adopted in December 2012 and effective on 7 January 2013, Fa Shi [2012] No. 24.

4. The legal facts for the establishment, alteration or termination of civil relationships occur outside the territory of the People's Republic of China.
5. Other circumstances subject to the determination.

The Interpretation supplements the Law of the People's Republic of China on the Laws Applicable to Foreign-related Civil Relations 2010 (hereafter 'the China Applicable Law for Foreign-related Civil Relations 2010').[183] The China Applicable Law for Foreign-related Civil Relations 2010 is considered to be the landmark legislation in the field of private international law as being the first single national codified law concerning the applicable law in relation to foreign-related civil relationships. It is enacted in order to clarify the application of laws concerning foreign-related civil relations, reasonably solve foreign-related civil disputes and safeguard the legal rights and interests of parties.[184] It employs consistent principles of 'party autonomy', 'habitual residence' and 'the closest relation' for the determination of the applicable law in accordance with China General Principles of Civil Law, China Civil Procedures Law and China Contract Law.

Party autonomy/freedom of choice

With regard to the applicable law in foreign contracts, the National People's Congress of the People's Republic of China enacted a unified Contract Law,[185] which has been in force since 1 October 1999. Article 126 of the China 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'.[186] Furthermore, Chapter VIII of General Principles of Civil Law of the People's Republic of China[187] determines which applicable law should be applied in civil relations with foreigners. 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 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'. In addition, the China Applicable Law for Foreign-related Civil Relations

183 Law of the People's Republic of China on the Laws Applicable to Foreign-related Civil Relations (hereafter 'the China Applicable Law for Foreign-related Civil Relations 2010'), issued by the Standing Committee of the National People's Congress, adopted on 28 October 2010 and effective on 1 April 2011, Order No. 36 of the President of the People's Republic of China.

184 China Applicable Law for Foreign-related Civil Relations 2010, Article 1.

185 China National People's Congress, Public Notice 1999 No. 14.

186 The China Contract Law 1999, Article 126.

187 General Principles of Civil Law of the People's Republic of China 1986, Articles 142–150.

2010 also specifies the principle of 'party autonomy' that 'the parties may explicitly choose the laws applicable to foreign-related civil relations in accordance with the provisions of law'.[188]

Applicable law in the absence of choice

In the absence of the parties' choice, the general rule of 'habitual residence' has been an underlying general principle for the determination of the applicable law for contractual relationships in the Chinese legal system. The China Applicable Law for Foreign-related Civil Relations 2010 explicitly affirms that 'the laws at the habitual residence shall apply to the civil rights capacities of a natural person',[189] and:

> the parties concerned may choose the laws applicable to contracts by agreement. If the parties do not choose, the laws at the *habitual residence* of the party whose fulfilment of obligations can best reflect the characteristics of this contract or other laws which have the closest relation with this contract shall apply.[190]

For B2C commercial contracts, the principle of 'habitual residence' is also the primary rule for the determination of applicable law. For example, the Article 42 of the China Applicable Law for Foreign-related Civil Relations 2010 provides that:

> A consumer contract is governed by the law of the consumer's habitual residence. Where the consumer chooses the law of the place where the commodity or the service is provided, or where the business operator does not engage in any business activity in the habitual residence of the consumer, the law of the place where the commodity or service is provided shall be applied.[191]

Where the general principle of 'habitual residence' cannot be determined, the principle of 'the closest relation' is employed to determine the applicable law for B2B contractual relationships. For example, Article 126 of the China 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'.[192] It then further tackles specific points, such as that 'the contracts for Chinese–foreign equity joint ventures,

188 China Applicable Law for Foreign-related Civil Relations 2010, Article 3.
189 China Applicable Law for Foreign-related Civil Relations 2010, Article 11.
190 China Applicable Law for Foreign-related Civil Relations 2010, Article 41.
191 China Applicable Law for Foreign-related Civil Relations 2010, Article 42.
192 The China Contract Law 1999, Article 126.

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'.[193]

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.[194]

The Supreme Court explains characteristic performance such 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.[195] 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 the 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 be then without the seller's 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.

The China Applicable Law for Foreign-related Civil Relations 2010 (Article 6) also confirms that 'as for the application of foreign laws on a foreign-related civil relation, if different laws are enforced in different regions of this foreign country, the laws of the region which has *the closest relation* with this foreign-related civil relation shall apply'.[196] It further clarifies the determination of 'the closest relation' for the applicable law in the absence of parties' choice, specifying that '[*L*]*ex fori* shall apply to the determination of the nature of foreign-related civil relations.'[197] In addition, it indicates relevant

193 Ibid.

194 M. Zhang (2006) 'Choice of law in contracts: a Chinese approach', *Northwestern Journal of International Law and Business*, 26: 289, at p. 325.

195 See Supreme People's Court, the Answers to Questions about Application of the Foreign Economic Contract Law of China (1987).

196 China Applicable Law for Foreign-related Civil Relations 2010, Article 6.

197 China Applicable Law for Foreign-related Civil Relations 2010, Article 8; *lex fori* means 'law of the place where the contract is made'; see also *Starr Printing Co.* v. *Air Jamaica*, 45 F.Supp.2d. 625 (1999 US Dist.).

connecting factors as to the determination of the place where the contract is made, stipulating that:

> The laws at *the locality of registration* shall apply to such items as the civil rights capacities, civil acts capacities, organizational institutions, rights and obligations of shareholders, etc. of a legal person and its branch.
>
> If the main business place of a legal person is inconsistent with the locality of registration, the laws of *the main business place* may apply. The main business place of a legal person shall be its *habitual residence*.[198]

In short, 'party autonomy' is the principle of ascertaining the applicable law, whereas 'closest connection', the same as in the EU and US, is the factor to determine the applicable law in the absence of choices. The closest connection to the contract concluded online should be the seller's place of business, and if not, his habitual residence.

Summary: a comparative study

In the EU, US and China, choice of law systems are all in favour of 'party autonomy' in general, though the interpretation and implementation of the concept of 'party autonomy' varies among them. In principle 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. The doctrine of 'habitual residence' has been commonly classified as a primary connecting factor for the determination of the 'closest relationship' or 'most closely connected' test for the place of business or performance. In the author's opinion, the place of business or performance is more difficult to determine in electronic transactions than in traditional paper-based communications. Generally, traditional choice of law principles should still apply to electronic contracts if the delivery of goods involves physical transfer. It is of great necessity to further establish or clarify the methods of determining the applicable law to Internet-related contractual disputes due to the complex and unique characteristics of online contracting when involving electronic delivery, 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 a choice-of-law clause, the law of the country which is most closely connected with an Internet-related contractual relationship should govern the contract. This will be determined by looking at the most closely connection factors: where the place of performance is (such as the

198 China Applicable Law for Foreign-related Civil Relations 2010, Article 14.

place of downloading or the location of implementing software apps) and whether the defendant has directed his business activities in a state which have effects in that state (such as digital products are designed to target consumers in a particular place/state). According to the findings in the EU, US and China, it appears that the seller's place of business or habitual residence is commonly deemed to be a primary connected factor for the determination of the applicable law for B2B electronic contracts in the absence of a choice-of-law clause, although this may lead to different results between the country where the law is chosen and the country where the court is located because a court in another country may have jurisdiction. It may raise concern over the inconsistency of the choice of court and choice of law findings in the absence of a conflict-of-law clause/agreement. For B2C electronic contracts, there is a consensus that the buyer's (consumer's) habitual residence should be in principle considered as a primary factor for the determination of the applicable law.

12.3 Online dispute resolution

In the 1980s, alternative dispute resolutions (ADR) were most commonly used to resolve international commercial transaction disputes other than cross-border litigation. ADR, including arbitration, mediation/conciliation and negotiation, is considered to be more efficient, flexible, confidential and less costly compared with traditional litigation. ADR can avoid the long court proceedings in international disputes which are affected by 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 and usage increased the probability of cross-border disputes. Parties situated in different continents may be opposed over small claims or cyber-related issues. Such kinds of dispute challenged the traditional dispute resolutions because of the following:

- Different countries have different rules for trade and various prohibitive costs for legal action across jurisdictional boundaries.
- The much less obvious localisation factor on the Internet causes 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.
- Cyber-related disputes may require a legal expert who is able to adapt to the diverse evolving technological, social nature and commercial practice of cyberspace.

In the process of creating a less costly but more efficient solution to resolve Internet-related disputes, the modernisation of ADR – online dispute resolution

(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 CyberTribunal Project at the University of Montreal, Canada.[199] It aims to provide more efficient, cost-effective and flexible dispute resolutions in the information society. ODR takes advantage of the Internet, a resource that extends what we can do, where we can do it and when we can do it.[200] 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, e-mail 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.[201]

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

The latest definition of ODR was proposed in the UNCITRAL Draft Procedural Rules on Online Dispute Resolution for Cross-border Electronic Commerce Transactions 2013 (Article 2(1)) as follows:

> 'ODR' means online dispute resolution which is a mechanism for resolving disputes facilitated through the use of electronic communications and other information and communication technology.[202]

12.3.1 Current legislation in the EU, US and China

The EU framework

In the EU, the use of ADR, in particular arbitration and mediation, is encouraged to resolve cross-border commercial disputes. The importance of arbitration

199 L. M. Ponte (2001) 'Throwing bad money after bad: can online dispute resolution (ODR) really deliver the goods for the unhappy Internet shopper?', *Tulane Journal of Technology and Intellectual Property*, 3: 55, at pp. 60–1.

200 E. M. Katsh and J. Rifkin (2001) *Online Dispute Resolution: Resolving Conflicts in Cyberspace* (San Francisco: Jossey-Bass), p. 10.

201 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 accessed 30 June 2013).

202 UNCITRAL Online Dispute Resolution for Cross-border Electronic Commerce Transactions: Draft Procedural Rules, A/CN.9/WG.III/WP.119, 11 March 2013.

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.[203] 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.'[204] As a result the Brussels I Regulation (Recast) 2012 excludes 'arbitration' by specifying that 'this Regulation shall not apply to arbitration'.[205]

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[206] and entered into force in June 2008.[207] 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.[208] 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

203 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 April 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 accessed 30 June 2013).

204 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 April 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 accessed 30 June 2013).

205 The Brussels I Regulation (Recast) 2012, Recital 12.

206 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 accessed 30 June 2013).

207 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, OJ L136/5, 24 May 2008. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:136:0003:0008:EN:PDF (last accessed 30 June 2013).

208 EU Press Release Reference: Mediation in Civil and Commercial Matters, MEMO/08/263, Brussels, 23 April 2008. Available at: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/08/263&type=HTML&aged=0&language=EN&guiLanguage=en (last accessed 30 June 2013).

process, which is reflected by Recitals 8 and 9 of the EC Directive on Mediation:[209]

> (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.[210]

Moreover, the provisions of 'ensuring the quality of mediation'[211] and 'information for the general public'[212] also indicate the support for using ODR methods 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 also explicitly encourages Member States 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 the EC Directive on Electronic Commerce does not provide substantial ODR rules, 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'.[213] 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'[214] 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'.[215]

On 21 May 2013 the European Parliament and the Council adopted the first regulation concerning ODR,[216] along with the EC Directive on Consumer

209 F. Wang (2008) *Online Dispute Resolution: Technology, Management and Legal Practice from an International Perspective* (Oxford: Chandos), p. 44.
210 EC Directive on Mediation 2008, Recitals 8 and 9.
211 EC Directive on Mediation 2008, Article 4.
212 EC Directive on Mediation 2008, Article 9.
213 EC Directive on Electronic Commerce 2000, Article 17(1).
214 EC Directive on Electronic Commerce 2000, Article 17(2).
215 EC Directive on Electronic Commerce 2000, Article 17(3).
216 Regulation (EU) No. 524/2013 of the European Parliament and the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No. 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR), OJ L165/1, 18 June 2013.

ADR.[217] The Regulation on Consumer ODR 2013 is considered to be landmark legislation, although it is only applicable to resolve consumer contractual disputes. It applies to 'the out-of-court resolution of disputes concerning contractual obligations stemming from online sales or service contracts between a *consumer* resident in the Union and a *trader* established in the Union'.[218] This regulation is adopted in response to a growing concern that:

> [F]ragmentation of the internal market impedes efforts to boost competitiveness and growth. Furthermore, the uneven availability, quality and awareness of *simple, efficient, fast and low-cost* means of resolving disputes arising from the sale of goods or provision of services across the Union constitutes a barrier within the internal market which undermines consumers' and traders' confidence in shopping and selling across borders.[219]

Consumers' confidence is so vital for online transactions that 'it is essential to dismantle existing barriers and to boost consumer confidence.'[220] It is possible that 'the availability of reliable and efficient online dispute resolution (ODR) could greatly help achieve this goal.'[221] To boost consumers' confidence, a mechanism should have the merits of being simple, reliable, efficient, fast and low-cost. These credentials are specified by Recital 8 as an addition to Recital 6 and also mirrored by the provision of the standard timeframe of resolving disputes as follows:

> Where the parties fail to agree within *30 calendar days* after submission of the complaint form on an ADR entity, or the ADR entity refuses to deal with the dispute, the complaint shall not be processed further. The complainant party shall be informed of the possibility of contacting an ODR advisor for general information on other means of redress.[222]

There are two key concepts involved in this Regulation: one is 'ODR' and the other is 'consumers'. The concept of 'consumers' is interpreted in Recital 13:

> The definition of 'consumer' should cover natural persons who are acting outside their trade, business, craft or profession. However, if the contract is concluded for purposes partly within and partly outside the person's

217 Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No. 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR), OJ L165/63, 18 June 2013.

218 EU Regulation on Consumer ODR 2013, Article 2(1).

219 EU Regulation on Consumer ODR 2013, Recital 4.

220 EU Regulation on Consumer ODR 2013, Recital 6.

221 EU Regulation on Consumer ODR 2013, Recital 6.

222 EU Regulation on Consumer ODR 2013, Article 9(8).

> trade (dual purpose contracts) and the trade purpose is so limited as not to be predominant in the overall context of the supply, that person should also be considered as a consumer.[223]

As to the concept of ODR, although there is no definition of ODR, the description of an ODR platform is given in this Regulation. The ODR platform is defined in Article 5(2) as:

> a single point of entry for consumers and traders seeking the out-of-court resolution of disputes covered by this Regulation. It shall be an interactive website which can be accessed electronically and free of charge in all the official languages of the institutions of the Union.[224]

According to this definition, the features of the ODR platform should be threefold: (1) a single point of entry at Union level; (2) an interactive website that is free of charge in all the official languages; (3) an out-of-court dispute resolution.[225] In order to create an ODR platform at Union level, each Member State is required to designate one ODR contact point.[226] The main ODR procedure includes 'submission of a complaint' (Article 8), 'processing and transmission of a complaint' (Article 9) and 'resolution of the dispute' (Article 10). It requires that parties have to agree on an ADR entity to deal with disputes.[227] Although ADR procedures vary in each ADR entity, the EC Directive on Consumer ADR 2013 has established harmonised quality requirements for ADR entities and ADR procedures.[228] In addition, protective measures are required to protect the database, the processing of personal data, data confidentiality and security. Finally, rules on effective, proportionate and dissuasive penalties are required to be specified by Member States.[229]

It is possible that the outcome of the ADR procedure by electronic means may be binding or non-binding, which depends on the ADR entity that parties agree upon at the beginning of the process as a description of the characteristics of each ADR entity includes the binding or non-binding nature of the outcome of the ADR procedure.[230]

After all, the adoption of the EU Regulation on Consumer ODR 2013 is the recognition of the benefit of using an ODR mechanism for consumers' contractual disputes of online transactions. This significant recognition and pioneer legislative model may be helpful for the future deployment and legal

223 EU Regulation on Consumer ODR 2013, Recital 13.
224 EU Regulation on Consumer ODR 2013, Article 5(2).
225 See also EU Regulation on Consumer ODR 2013, Recital 18.
226 EU Regulation on Consumer ODR 2013, Article 7(1).
227 EU Regulation on Consumer ODR 2013, Article 9(3).
228 EC Directive on Consumer ADR 2013, Article 2(3).
229 EU Regulation on Consumer ODR 2013, Article 18.
230 EU Regulation on Consumer ODR 2013, Article 9(5)(e).

transplantation of an ODR mechanism in other fields such as B2B contractual transactions, financial services or other types of small claim disputes.

The US trend

In the US, there is no uniform legislation regulating ODR services. Self-regulation and guidelines of best practice are the approaches recommended by the American Bar Association (ABA). 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'.[231] The ABA essentially recommends best practices to ODR providers in that they should adhere to adequate standards and codes of conduct and strive to achieve transparency through information and disclosure as a basis to attain sustainability.[232] A non-profit, educational and informational entity, the iADR Center, 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,[233] which specified nine standards of conduct for mediators: 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 offers fast, convenient online claim filing through their AAA WebFile® service known as an ODR platform, which includes functions such as filing claims, making payments, performing online case management, accessing rules and procedures, electronically transferring documents, selecting neutrals, using a case-customised message board and checking the status of their case.[234] In 2010 AAA's international division – the International Center for Dispute Resolution (ICDR)) – introduced a Manufacturer/Supplier Online Dispute Resolution Protocol for Manufacturer/Supplier Disputes (known as 'the MS-ODR Program').[235] The MS-ODR program is designed to help manufacturers and suppliers to resolve small disputes (the total amount does not exceed US$10,000) quickly, fairly and inexpensively in order to move on with their business relationship. There are two phases in the process: negotiation and arbitration. At the end a dispute is either settled or decided by an arbitrator.

231 ABA ODR Survey (2002).

232 ABA ODR Survey (2002), at p. 444.

233 ABA Model Standards of Conduct for Mediators, September 2005. Available at: http://www.abanet.org/dispute/documents/model_standards_conduct_april2007.pdf (last accessed 30 June 2013).

234 AAA Webfile. Available at: https://apps.adr.org/webfile/ (last accessed 30 June 2013).

235 The ICDR Manufacturer/Supplier Online Dispute Resolution Protocol: MS-ODR Programme. Available at: http://www.adr.org or http://www.icdr.org (last accessed 30 June 2013).

The entire process is designed to take no longer than 66 days.[236] The online negotiation uses the 'double blind bidding' system created by CyberSettle, a strategic alliance with AAA, and if the dispute does not settle within the 12 days of the online negotiation, it then proceeds to the next stage of online arbitration.

In addition, the list of circuit courts providing eFiling services in the US continues to grow. For example, the latest eFiling service was employed by the Jackson circuit court in Oregon on 3 June 2013 which was the fourth circuit court that joined the eCourt service since the deployment of the Oregon eCourt in June 2012.[237]

The Chinese approach

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.[238] It requires that 'an arbitration agreement shall include the arbitration clauses provided in the contract and *any other written form* of agreement concluded before or after the disputes providing for submission to arbitration'.[239] The form requirement of 'any other written form' requires further interpretation in that the arbitration clauses concluded by electronic means are equivalent to the 'written form'.

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,[240] conditions for arbitrators' appointment[241] and requirements of establishment.[242]

To harmonise the standard of online arbitration practice in China, the 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 the resolution of disputes over electronic commerce transactions, and other economic and trade disputes in

236 ICDR Manufacturer/Supplier Online Dispute Resolution Program (Frequently Asked Questions). Available at: http://www.icdr.org (last accessed 30 June 2013).

237 Oregon eCourt Implementation News. Available at: http://courts.oregon.gov/oregonecourt/Pages/index.aspx (last accessed 30 June 2013).

238 Arbitration Law of the People's Republic of China (hereafter 'China Arbitration Law'), adopted at the 8th Session of the Standing Committee of the 8th National People's Congress and promulgated on 31 August 1994.

239 China Arbitration Law 1994, Article 16.

240 China Arbitration Law 1994, Article 10.

241 China Arbitration Law 1994, Article 13.

242 China Arbitration Law 1994, Article 11.

which the parties agree to apply these Rules for dispute resolution.[243] 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.

Different from arbitration, mediation is used in commercial dispute resolution to maintain ongoing business relationships.[244] The Chinese legislation is in support of mediation in civil and commercial disputes. For example, Article 51 of the Civil Procedure Law permits the parties to 'reach a compromise of their own consent'.[245] Article 49 of the China Arbitration Law stipulates that parties may reach a private settlement even after the commencement of arbitration proceedings.[246] Article 25 of the Law of the People's Republic of China on Chinese-foreign Contractual Joint Ventures[247] 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.

As to international harmonisation, 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').[248] The New York Convention is considered to be one of the most successful conventions, which gives the certainty of recognition and enforcement of cross-border arbitral award. As the New York Convention was adopted well 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 are capable of meeting the requirements of the written form under the New York Convention. It is suggested that if the digital

243 CIETAC Online Arbitration Rules 2009, Article 1.

244 J. Tao (2005) *Resolving Business Disputes in China*, Asia Business Law Series (Leiden: Kluwer Law International), pp. 1012–13.

245 China Civil Procedure Law 1991, Article 51.

246 China Arbitration Law 1994, Article 49.

247 Law of the People's Republic of China on Chinese-foreign Contractual Joint Ventures, adopted by the First Session of the Standing Committee of the Seventh National People's Congress on 13 April 1988, which was promulgated and revised by the Eighteenth Session of the Standing Committee on the Ninth National People's Congress on 31 October 2000.

248 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 accessed 30 June 2013).

arbitral awards can be printed and signed, it would satisfy the written requirement. The electronic arbitration agreements and arbitral awards are considered to be equivalent to the effect of electronic contracts. Subsequently the effectiveness of arbitration clauses/agreements concluded by electronic means will be recognised by the UN Convention on the Use of Electronic Communications in International Contracts 2005 and other relevant national laws concerning electronic commerce. Moreover, the UNCITRAL Model Law on International Commercial Arbitration 1985, with amendments as adopted in 2006, explicitly recognises the effectiveness of an arbitration agreement concluded by electronic communications if the information contained therein is accessible so as to be useable for subsequent reference.[249]

With regard to eCourt systems, in recent years the list of national and local courts providing eCourt services in China has been growing. For example, Zhejiang Province eCourt system has been employed for online litigation filings since 2011.[250] Shanghai courts have also adopted the eCourt system facilitating litigation procedures online.[251]

12.3.2 Successful pioneer examples of global ODR services

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

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

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, and was created in 1999. Both eBay and SquareTrade are independent private companies. Although

249 UNCITRAL Model Law on International Commercial Arbitration 1985, with amendments as adopted in 2006, Article 7(4).

250 Zhejiang eCourt System. Available at: http://www.zjcourt.cn:8088/wsla/login.jsp?fydm=330000 (last accessed 30 June 2013).

251 Shanghai Courts eFiling Service. Available at: http://www.hshfy.sh.cn/shfy/gweb/zxfw.jsp (last accessed 30 June 2013).

they are engaged in different Internet industries, they have a common aim of promoting customer 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 in buying and selling online so that a maximum number of sellers and buyers will be attracted to its online marketplace. eBay's trust-building measures 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 last but not least (5) the ODR service provided by SquareTrade.

SquareTrade, eBay's preferred dispute resolution provider, helps eBay users who have disputes over eBay transactions. SquareTrade's position is practically that of an in-house dispute resolution provider as eBay refers its users exclusively to SquareTrade though 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.[252] This second stage is called 'online mediation'.

The usage of SquareTrade by eBay benefits the resolution of misunderstandings fairly, providing a neutral go-between for buyers and sellers, reducing premature negative feedback and generating trust in the eBay community.[253]

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.[254] 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 profound reputation and exclusive merits in their fields.

On 2 October 2006 the AAA and Cybersettle announced a strategic alliance that would provide clients of both companies with the opportunity to use the dispute resolution services of both companies exclusively. With the goal of 'ensuring that no one walks away without a resolution', said Cybersettle

252 Dispute Resolution Overview. Available at: http://pages.ebay.com/services/buyandsell/disputeres.html (last accessed 30 June 2013).

253 Dispute Resolution Overview. Available at: http://pages.ebay.com/services/buyandsell/disputeres.html (last accessed 30 June 2013).

254 About us (AAA). Available at: http://www.adr.org/about (last accessed 30 June 2013).

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.[255]

This strategic alliance not only makes full use of the reputation and merits of both parties, but also takes advantages of their different successful experiences. For example, the 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.[256]

The AAA, an experienced public sector organisation, cooperates with Cybersettle, a young enthusiastic private sector organisation, which could provide a model or a good strategic plan for the development of the ODR industry. The AAA's professional regulations, such as the 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. The AAA's dispute resolution 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 the 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 Organisation (WIPO) are both public international organisations but with different functions. ICANN is responsible for managing the generic top-level domains and was in urgent need of a solution to the dispute resolution problem,[257] while WIPO is responsible for developing a balanced and accessible international intellectual property (IP) system.[258]

255 Information about AAA and Cybersettle Sign Unique Partnership Agreement. Available at: http://www.adr.org/sp.asp?id=32533 (last accessed 30 June 2013).

256 Industry New: New Joint Dispute Resolution Service Ready to Launch. Available at: http://www.adr.org/sp.asp?id=29624 (last accessed 30 June 2013).

257 The Internet Corporation for Assigned Names and Numbers (ICANN). Available at: http://www.icann.org/ (last accessed 30 June 2013).

258 'What is WIPO?'. Available at: http://www.wipo.int/about-wipo/en/what_is_wipo.html (last accessed 30 June 2013).

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 timely and cost-efficient arbitration and mediation in cross-border dispute settlement.[259]

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.[260] Since then, the WIPO Centre has been providing ODR services for resolving domain name disputes and has administered over 30,000 proceedings, of which over 15,000 cam under the WIPO-UDRP adopted by ICANN.[261]

In December 2008 WIPO submitted a proposal for an 'eUDRP Initiative'[262] 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 e-mail in order to eliminate the use of vast quantities of paper and improve the timeliness of UDRP proceedings without prejudicing either complainants or respondents.[263]

Scholars have identified the reasons for the success of the WIPO-UDRP domain name dispute resolution system, such as credibility, transparency, self-enforcement, accountability, etc.[264] Firstly, WIPO and ICANN are both pubic organisations with authority. 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,[265] which increases the *transparency* of the procedure

259 The WIPO Arbitration and Mediation Center. Available at: http://www.wipo.int/amc/en/index.html (last accessed 30 June 2013).

260 Frequently Asked Questions: Internet Domain Names. Available at: http://www.wipo.int/amc/en/center/faq/domains.html (last accessed 30 June 2013).

261 WIPO Advanced Workshop on Domain Name Dispute Resolution: Update on Practices and Precedents, WIPO, Geneva, Switzerland, 13 and 14 October 2009. Available at: http://www.wipo.int/amc/en/events/workshops/2009/domainname/ (last accessed 30 June 2013).

262 WIPO eUDRP Initiative. Available at: http://www.wipo.int/export/sites/www/amc/en/docs/icann301208.pdf (last accessed 30 June 2013).

263 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 accessed 30 June 2013).

264 P. Motion (2005) 'Article 17 ECD: encouragement of alternative dispute resolution. On-line dispute resolution: a view from Scotland', in L. Edwards (ed.), *The New Legal Framework for E-commerce in Europe* (Oxford: Hart), pp. 137–69, at p. 148.

265 WIPO UDRP Domain Name Decision (gTLD). Available at: http://www.wipo.int/amc/en/domains/decisionsx/index.html (last accessed 30 June 2013).

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 ten days after the decision is rendered.[266] 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.[267] The supplementary rule of the 'eUDRP initiative' reflects 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. Hong Kong is the only economy with a common law tradition incorporated with English case law (before 1997) in the Greater China Area.[268] It means that the laws in Hong Kong will be different from those in China. The business link between China and Kong Kong is very close. A large number of companies have their headquarters in China but branches in Kong Kong, or vice versa. If a company registers a '.com or .net' domain name and has offices in both mainland 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 Hong Kong International Arbitration Centre (HKIAC) to deal with gTLD (.com/.org) domain name disputes.[269] The Asian Domain Names Dispute Resolution Centre has two offices in Beijing and Hong Kong. Both offices comply with the same policy – WIPO UDRP for gTLD disputes. Complainants can choose one or other 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) to provide dispute resolution services with regard to .cn domain names, known as the 'CIETAC Domain Name Dispute Resolution Centre'[270] and

266 UDRP Policy, Paragraph 4(k).

267 Case filing under the UDRP. Available at: http://www.wipo.int/amc/en/domains/filing/udrp/index.html (last accessed 30 June 2013).

268 J. Mo (2013) 'Developing uniform rules for commercial contracts in Greater China', *Uniform Law Review*, 18: 128–53, at pp. 133–4.

269 Asian Domain Name Dispute Resolutions Center. Available at: http://www.adndrc.org/adndrc/index.html (last accessed 30 June 2013). Please note that it also includes the Korean Internet Address Dispute Resolution Committee (KIDRC).

270 CIETAC Domain Name Dispute Resolution Center. Available at: http://dndrc.cietac.org/static/english/engfrmain.html (last accessed 30 June 2013).

the 'HKIAC .cn Domain Name Resolution Centre'.[271] The .cn domain name disputes are carried out under the CNNIC Domain Name Dispute Resolution Policy (CNDRP)[272] 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 e-mail.[273] 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.[274] The panel's decision will be submitted both in electronic and paper form signed by all the panellists. The decision will be published on the websites of the service providers except in special circumstances.[275]

For example, the case *Avon Products, Inc.* v. *Ni Ping*[276] was filed with the ADNDRC Beijing Office on 27 April 2007. The complainant is one of the world's most well known direct sellers of cosmetic products. Since 1886, the claimant claimed that 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 the registration of these trademarks throughout the world, including mainland China, Hong Kong, Taiwan and Singapore. It entered into the People's Republic of China (PRC) market in 1990 and now has 77 branches in China and over 6,000 specialty shops, while 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 the domain name 'yafang.net', which was registered on 12 August 2003 in Beijing, would confuse existing and future customers of the claimant 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

271 HKIAC .cn Domain Name Resolution Center. Available at: http://dn.hkiac.org/cn/cne_welcome.html (last accessed 30 June 2013).

272 The China Internet Information Center (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.

273 Hong Kong International Arbitration Centre (HKIAC). Available at: http://dn.hkiac.org/cn/cne_complaint_form.html (last accessed 30 June 2013).

274 Rules for CNNIC Domain Name Dispute Resolution Policy, Article 37. Available at: http://dn.hkiac.org/cn/cne_rules_procedure.html (last accessed 30 June 2013).

275 Rules for CNNIC Domain Name Dispute Resolution Policy, Article 44. Available at: http://dn.hkiac.org/cn/cne_rules_procedure.html (last accessed 30 June 2013).

276 *Avon Products, INC.* v. *Ni Ping,* CN-0600087. Available at: http://www.adndrc.org/adndrc/bj_statostocs.html (last accessed 30 June 2013).

the link to '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 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 generates consistency, harmony and certainty.

Summary: lessons to be learned

eBay and SquareTrade, AAA and Cybersettle, ICANN and WIPO-UDRP, CIETAC and HKIAC are four successful examples of international ODR practices which provide a tremendous amount of valuable experience.

Firstly, they provide advanced technology support and make a very attractive offer for easy 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.[277] The mediation process on SquareTrade for eBay users generally takes only ten days.[278]

Secondly, they have succeeded in integrating their offer into the primary markets.[279] The four ODR services mainly target the resolution of e-commerce-related disputes; for example, the SquareTrade dispute resolution service provider deals with eBay users' online trading disputes, while WIPO-UDRP or CIETAC and HKIAC deal with ICANN domain name users' disputes.

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

277 Dispute Resolution Overview. Available at: http://pages.ebay.com/services/buyandsell/disputeres.html (last accessed 30 June 2013).

278 Dispute Resolution Overview. Available at: http://pages.ebay.com/services/buyandsell/disputeres.html (last accessed 30 June 2013).

279 G. P. Calliess (2006) 'Online dispute resolution: consumer redress in a global market place', *German Law Journal*, 7 (8): 647, at p. 653.

Fourthly, the ODR service is promoted by creating socio-legal bonds for potential dispute parties to commit to the process.[280] That is, the ICANN UDRP administrative procedure is mandatory for domain name holders, while the SquareTrade mediation process is mandatory for 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 a self-enforcement mechanism. The ICANN accredited-registrars have the right to transfer or cancel a domain name directly when the settlement decision is made.[281]

Sixthly, the ODR service has an advantage in that it is able to provide expertise in the resolution of certain Internet disputes, such as cross-border small-claim disputes and domain names disputes. The growth in the use of domain names appears to have increased the number of registrations in bad faith and further raised concerns that trademark owners' rights are increasingly being infringed or diluted by the use of trademarks in domain names.[282] That is, domain names have come into conflict with trademarks. The main reason for such conflict can be attributed to the lack of connection between the system of registering trademarks and the registration of domain names. The former is a system granting territorial rights enforceable only within the designated territory, while the latter is a system of granting rights that can be enforced globally.[283] Because trademark law is territorial, a mark may be protected only in the geographic location where it distinguishes its goods or services. Thus trademark 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.[284] Only one entity in the world can own the right to use a specific domain name that can be accessed globally.[285] According to the specific feature of the

280 In the author's perspective, 'social-legal bonds' refers to the combination of the powers of 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 at: http://odrworkshop.info/papers2005/odrworkshop2005Bol.pdf (last accessed 30 June2013).

281 Available at: http://www.icann.org/tlds/agreements/name/registry-agmt-appl-03jul01.htm (last accessed 30 June 2013).

282 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 accessed 30 June 2013) (hereafter 'Australian DR Review').

283 D. Tunkel and S. York (2000) *E-commerce: A Guide to the Law of Electronic Business*, 2nd edn (London: Butterworths).

284 F. Wang (2006) 'Domain names management and legal protection', *International Journal of Information Management*, 26 (2): 116–27, at p. 119.

285 Z. Efroni (2002) 'The Anticybersquatting Consumer Protection Act and the Uniform Dispute Resolution Policy: new opportunities for international forum shopping?', *Columbia Journal of Law and the Arts*, 26: 335–43, at p. 343.

non-territorial restriction to the usage of a domain name registered with any registrar in any country, ODR will be one of the most suitable methods to resolve domain names disputes.

12.3.3 The future of ODR: international standardisation

ODR not only provides speedy and cost-effective techniques 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.[286] 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 a measure to enhance the quality of its services. It may be possible to reach international standardisation through the promulgation of regulations, codes of conduct, guidelines, frameworks, model laws or even convention by international legislative organisations.

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

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 – these factors 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.[287] 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 service. The ODR service provider should clearly

286 F. Wang (2008) *Online Dispute Resolution: Technology, Management and Legal Practice from an International Perspective* (Oxford: Chandos), p. 61.

287 E. M. Katsh and J. Rifkin (2001) *Online Dispute Resolution: Resolving Conflicts in Cyberspace* (San Francisco: Jossey-Bass), p. 76.

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 in accord with 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*,[288] 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 in the morning following the mediation, he agreed to the settlement made in 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.[289] 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 kind of mediation agreement can be achieved by way of 'a court or other competent authority in a judgment or decision or in an authentic instrument'.[290] The EC Directive on Consumer ADR in 2013 also provides that 'in ADR procedures which aim at resolving the dispute by imposing a solution, the solution imposed should be binding on the parties only if they were informed of its binding nature in advance and specifically accepted this.'[291]

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 to be 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 resolving the dispute face to face. The EC Directive on Mediation supports

288 *Brown* v. *Rice*, [2007] EWHC 625 (Ch); [2007] BPIR 305 (Ch D).
289 EC Directive on Mediation 2008, Recital 19 and Article 6.
290 EC Directive on Mediation 2008, Article 6(2).
291 EC Directive on Consumer ADR 2013; see also Article 9(5)(e), EU Regulation on Consumer ODR 2013, Recital 43.

the enhancement of the confidentiality of mediation[292] by preventing mediators or those involved in the mediation process from giving information or evidence in civil and commercial judicial proceedings or arbitration.[293] The EU Regulation on Consumer ODR 2013 also affirms 'confidentiality' as a primary principle along with 'security'.[294] 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 the pre-agreement with users.

SquareTrade provides a good pioneer experience in balancing the right of confidentiality and accountability. As discussed, accountability hinges on transparency[295] and structure, while mediation's strength is drawn, to a large extent, from its confidentiality and flexibility.[296] 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 the other data information through the seal programme and users' registration. SquareTrade also records 'Resolution Behaviour Information' at the end of the ODR service, which is comprised of 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.[297] Such kind of data will be kept confidentially, but the outcome of statistics can be used in the market promotion analysis of the ODR service.

4. ODR service providers shall ensure, by any means which they consider appropriate, the availability to the general public of the code of conduct of ODR service, including administrative duties and procedures.

It should include, as recommended by the ABA Task Force on E-commerce and the ADR Recommended Best Practices for Online Dispute Resolution Service Providers: (a) publishing statistical reports; (b) employing identifiable

292 EC Directive on Mediation 2008, Recital 23 and Article 7.

293 EC Directive on Mediation 2008, Article 7(1).

294 EU Regulation on Consumer ODR 2013, Article 13.

295 On 11 July 2013, the United Nations Commission on International Trade Law (UNCITRAL) adopted the UNCITRAL Rules on Transparency in Treaty-based Investor-State Arbitration (the 'Transparency Rules'), UNIS/L/186.

296 O. Rabinovich-Einy (2006) 'Technology's impact: the quest for a new paradigm for accountability in mediation', *Harvard Negotiation Law Review*, 11: 253, at p. 256.

297 Square Trade Privacy Policy – Information We Collect (Item 4). Available at: http://www.squaretrade.com/privacypolicy (last accessed 30 June 2013).

and accessible data formats; (c) presenting printable and downloadable information; (d) publishing decisions with whatever safeguards to prevent party identification; (e) describing the types of services provided; (f) affirming due process guarantees; (g) disclosing minimum technology requirements to utilise the provider's technology; (h) disclosing all fees and expenses to use ODR services; (i) disclosing qualifications and responsibilities of neutrals; (j) 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.[298]

5. ODR service providers shall encourage, by any means appropriate, the use of Trust Mark Schemes in the online trading or service and voluntarily provide out-of court dispute resolutions to those disputes. Such scheme is 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 programmes or directly offering seal programmes. For example, the SquareTrade seal programme is a distinctive eBay service. Under this system, SquareTrade 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 sellers'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.[299]

From the examination of the four successful examples of e-Bay with SquareTrade, the AAA with Cybersettle, ICANN with WIPO-UDRP, as well as CIETAC and HKIAC, it can be suggested that the corporate agreement of ODR service providers and primary market makers, the expertise of technological and legal issues in Internet-related disputes and 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.

At the international level, since December 2010 the UNCITRAL Working Group III has been drafting the procedure rules on Online Dispute Resolution

298 'Recommended Best Practices by Online Dispute Resolution Service Providers'. Available at: http://www.abanet.org/dispute/documents/BestPracticesFinal102802.pdf (last accessed 30 June 2013).

299 O. Rabinovich-Einy (2006) 'Technology's impact: the quest for a new paradigm for accountability in mediation', *Harvard Negotiation Law Review*, 121: 253, at p. 259.

for Cross-border Electronic Transactions.[300] There was debate over whether such an instrument should be applicable to B2B electronic transactions only or follow a two-track implementation system (B2B and B2C).[301] In general the UNCITRAL Draft Procedural Rules for the Online Dispute Resolution for Cross-border Electronic Commerce Transactions proposed a standard as to the timing and process of notice and response in an ODR procedure.[302] It was suggested that substantive principles for ODR claims and relief should also be incorporated into Article 4 of the Draft Procedural Rules.[303]

In the author's view, international ODR guidelines are needed to harmonise the standard of ODR service in the global market. A sophisticated international instrument should clarify at least five main doctrines for regulating ODR as evaluated earlier in addition to a procedure rule on notice and response. They are: the appropriation and interoperability of ODR technology, the protection of confidentiality, the conditions of enforceability, the requirements of ODR administration and the implementation of trust mark schemes.

A harmonised international guideline on ODR principles and procedures will be beneficial to national legislative organisations for the establishment of a single national ODR regulation, or the amendment and update of the offline ADR rules and regulations by recognising electronic means of communication in resolving disputes and incorporating ODR concepts.

300 Working Group III: Online Dispute Resolution. Available at: http://www.uncitral.org/uncitral/commission/working_groups/3Online_Dispute_Resolution.html (last accessed 30 June 2013).

301 Report of Working Group III (Online Dispute Resolution) on the Work of Its Twenty-Seventh Session. New York, 20–24 May 2013; A/CN.9/769, 3 June 2013.

302 UNCITRAL Online Dispute Resolution for Cross-border Electronic Commerce Transactions: Draft Procedural Rules, A/CN.9/WG.III/WP.119, 11 March 2013.

303 Report of Working Group III (Online Dispute Resolution) on the Work of Its Twenty-Fifth Session. New York, 21–25 May 2012; A/CN.9/744, 7 June 2012.

Part IV Summary

Harmonisation of the rules of international jurisdiction and applicable law for Internet-related commercial transactions may be helpful to increase the legal certainty of litigation and balance the potentially conflicting interests of parties in different countries. However, the process of international harmonisation takes a long time due to the constraints of different interests and legal systems in countries and reliance on experiences from new industries. In the author's view, a well-balanced action plan for a modern private international law should include measures to:

- stimulate global economic growth without jeopardising technological innovation and market development;
- strike a balance of interests among contracting parties in electronic communications;
- standardise conflict-of-law agreements concluded by electronic means in terms of the formality and effectiveness;
- specify unique connecting factors for the determination of jurisdiction and applicable law for Internet-related disputes; and
- facilitate cross-border enforcement.

It is likely that sophisticated eCourt systems may also assist in promoting coordination between nations. Countries should be encouraged to share the best practices of eCourt systems and adopt appropriate technical measures in such systems.

Compared with court litigation, out-of-court dispute resolutions (both ADR and ODR) should be considered as simpler and more efficient means to deal with smaller claims of Internet-related disputes provided that there is harmonised quality and standard in ADR and ODR procedures.

This page intentionally left blank

Part V
The Future

This page intentionally left blank

13 Conclusions and recommendations

13.1 Future legislative trends in the EU, US and China

The advent of information technology infuses new patterns into the operation of commercial enterprises and 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 induced an explosion of electronic commerce. The rapid development of new technology constantly challenges the existing legal concepts and their application.

Broadly, the law of electronic commercial transactions is to promote free and fair trade between nations and within nations. In a narrow scope, the law of electronic commercial transactions is to regulate the conduct of businesses and individuals on the Internet and ensure the effectiveness of online commercial activities. The law of electronic commercial transactions relates to the fields of traditional contract law, international commercial law, private international law and alternative dispute resolution, covering wide-ranging legal issues. The cornerstone in this context is the legal recognition of the validity and effectiveness of contracts and agreements concluded by electronic means because traditional laws were promulgated before the widespread use of electronic commerce and without consideration of the usage of electronic means. The non-territory features in open networks accelerate other legal issues concerning signatory authentication, technical safeguards, data privacy protection, international jurisdiction and applicable law.

International, regional and national legislative organisations have been making efforts in producing a variety of particularised legal instruments to facilitate the development of electronic commerce. There are different approaches adopted in those organisations equipped for different social, historical, cultural, economic and political contexts. 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 to keep up

with the international standard when revising existing national laws and issuing supplementary legislative measures. During this ongoing legislative process in the law of electronic commercial transactions, nations have faced some common issues.

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 new, 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 this approach would avoid confusion and unnecessary complication of the legal system, it is debatable whether the traditional laws are sufficient and efficient enough to deal with newly emerging e-disputes. For example, the UN Convention on the Use of Electronic Communications in International Contracts (hereafter 'the UN Convention') 2005 does not govern substantial contractual issues. In the EU there is no single uniform electronic contract law; however, new legislative proposals such as the Common European Sales Law include substantial legal issues concerning electronic contracts. In contrast, in China the Ministry of Commerce of the People's Republic of China proposed a single legislative instrument – Regulatory Specifications on the Use of Online Signing Process in Electronic Contracts in 2012, together with the Qualification Standard for Electronic Commerce Enterprises.[2]

Secondly, the majority of transnational electronic transactions involve people that will never physically meet. In particular, with the rapid development of technologies, businesses and individuals are uncertain how, when and where personal data is collected, processed and stored in new smart devices or new network-based systems such as service-oriented computing and cloud computing. How to create trust and establish confidence in online interactions and transactions is challenging for national, regional and international lawmakers. Promoting trust and confidence in electronic commerce is one of the prioritised aims in the law of electronic commercial transactions. Following the initiatives of promoting confidence in electronic commerce by UNCITRAL in 2007,[3] the European Commission proposed a Regulation on Electronic

1 J. H. Dalhuisen (2007) *Dalhuisen on Transnational and Comparative Commercial, Financial and Trade Law*, 3rd edn (Oxford and Portland, OR: Hart), p. 254.

2 Circular of the Ministry of Commerce of the People's Republic of China, on Soliciting Comments on the Regulations of Online Signing Process of Electronic Contract (Draft), and Circular of the Ministry of Commerce of the People's Republic of China, on Soliciting Comments on Qualification Standard for Electronic Commerce Enterprise (Draft), the Ministry of Commerce, *China Foreign Trade and Economic Cooperation Gazette* (Issue No. 63 2012), October 2012. Available at: http://english.mofcom.gov.cn/article/policyrelease/gazette/201301/20130100015518.shtml (last accessed 30 June 2013).

3 2007 – Promoting Confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods (hereafter 'Promoting Confidence in Electronic Commerce 2007'), the United Nations Commission on International Trade Law (UNCITRAL), Vienna, United Nations, released in 2009. Available at: http://www.uncitral.org/pdf/english/texts/electcom/08-55698_Ebook.pdf (last accessed 30 June 2013).

Identification and Trust Services for Electronic Transactions in the Internal Market in 2012.[4]

Harmonisation or convergence of nation laws, whether by international conventions or model laws, conscious or unconscious judicial parallelism or uniform rules for specified types of contract may gradually remove the obstacles to 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 embedding the principle of technological neutrality so as to adapt to the future development of new technologies in electronic commercial transactions. From the research in this book there is strong evidence showing that electronic commercial transactions do have unique characteristics. The general concept of electronic commercial transactions is the same as the traditional one in that the process involves selling, buying, payment and delivery, but the actual conduct of the process of electronic transactions is fundamentally different. The process of electronic transactions may involve new software apps, smart devices, parties and subject matters (i.e. data).

It is certain that electronic transactions can be considered to be a means of communication from a technological point of view. 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',[5] and 'the place of business'[6] in cyberspace. When digitised/intangible goods with online delivery are involved, these two factors, as explained in the chapters above, 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 become insufficient to govern these issues.

It is noteworthy that before drafting completely new electronic commerce laws, careful consideration should be given to existing laws. If nations decide not to produce new single statutes on electronic commerce or electronic contracts, it is recommended that those nations adopt the international instruments in electronic commerce in order to promote international trade relationships. An explanatory note to the existing laws should also be 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

4 Proposal for a Regulation of the European Parliament and of the Council on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market, COM/2012/0238 final – 2012/0146 (COD), Brussels, 4 June 2012.

5 UN Convention on the Use of Electronic Communications in International Contracts 2005 (hereafter 'the UN Convention'), Article 10.

6 The UN Convention 2005, Article 6.

commerce into existing laws as well as modernise the existing provisions, or create new sets of laws in electronic commercial transactions.

Legal issues relating to technologically specific areas such as electronic signatures and authentication and the conduct/procedures of online dispute resolution (ODR) shall be encouraged to accept regulation in a separate set of laws, because using electronic means creates new concepts, raises new issues and challenges the effectiveness of agreements and the validity of evidence in legal proceedings, although the form requirements of contracts and signatures and the generic process of litigation and alternative dispute resolution (ADR) remain the same.

Most nations have made efforts to remove legal barriers to electronic commerce and adapt to the ever-changing technological environment. International legislative organisations push forward the process of harmonisation of international electronic commerce proposing general principles to create confidence for doing business online. However, some legal obstacles to electronic commercial transactions remain unresolved through lack of substantive rules in law.

13.2 Solutions to the obstacles in the law of electronic commercial transactions

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

The first solution concerns the determination of electronic offer and acceptance and the valid incorporation of terms and conditions in electronic contracts. After examining the characteristics of electronic communications, including e-mail 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 almost instantaneous. Although dispatching an e-mail is like dropping a letter in a red post box, e-mail communication is still 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 to the receipt of an offer and acceptance. Therefore the postal rule loses its original purposes and traditional functions 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, in electronic communications, the acceptance should be effective when it is retrieved or read by the offeror within a reasonable time provided that the addressee is aware that the acceptance has been sent to that address.

As to the incorporation of terms and conditions into contracts by electronic means, making terms and conditions available in a clear, appropriate and comprehensive way is a prerequisite to the effectiveness of incorporating

terms and conditions into contracts in electronic communications. Thus there is a need to implement a harmonised standard of 'the availability of terms and conditions' in electronic communications at the national, regional and international levels. According to the current EU, US and Chinese legislation, it is a common requirement that the T&C should be capable of being downloaded, re-accessed or reprinted for subsequent reference, although some regions (such as the EU) require that 'information is provided on a durable medium' with regard to distance contracts for consumers.[7] The traditional methods of incorporation of contract terms by signatures, by notice/reference and by course of dealing (or by custom) can be employed in electronic communications as long as they meet the form requirements as to the validity of electronic signatures, the availability of contractual terms and informed consent. Failure to comply with these requirements is usually subject to relevant national laws.

The second solution refers to removing the legal barriers on error in electronic communications and the battle of the forms. With regard to error in electronic communications, appropriate technical measures should be made available to amend or withdraw error in electronic communications. 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. In the information society, error in electronic communications usually refers to input mistakes or the input of a false statement (misrepresentation) by electronic means. The determination of mistake and misrepresentation occurring in electronic communications should be in theory similar to that at the time of forming a traditional contract, although specific interpretation of traditional concepts may be required to adapt to the new characteristics of an online error. The UN Convention requires '(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 of value from the goods or services.'[8] In the EU, US and China, it is also a common rule in the duty of promptly notifying an error, taking reasonable steps provided that there is non-use of, or non-benefit from, the goods. There is a need to define the timeframe of notification of error in electronic communications (i.e. within 24 hours) to ensure fairness and appropriateness of the process, taking into account the new functional development of technology (such as 'recall or replace a message').

With regard to the battle of the forms, there are at least three prerequisites for the determination of which form should prevail and which battle should win in an electronic contracting environment. The first prerequisite is the appropriate and effective manner of making contractual terms available in electronic forms. The second prerequisite is the appropriate technical measures

7 EC Directive on Consumer Rights 2011, Article 8(1).
8 The UN Convention 2005, Article 14.

provided for correcting an input error in electronic communications. The third prerequisite is the intention of the parties with regard to forming a contract by electronic means but not merely communicating an inquiry by electronic means. The harmonisation of the determination of an electronic battle of forms may be achieved by the amalgamation of the traditional 'battle of forms' rules in the international legislation (such as the CISG and UNIDROIT Principles) and the modern 'electronic communications' rules in the UN Convention or other relevant regional and nation laws in practice. It is inevitable that an electronic acceptance that contains additions, limitations or other modifications may be a rejection of the offer and constitute a counter-offer. 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 parties agree. This should apply where parties have met the three prerequisites for forming a contract in an electronic contracting environment.

The third solution focuses on the removal of barriers to the recognition of electronic signatures, authentication and certificates, in particular cross-border recognition and interoperability. Electronic signature is essential because it identifies the contracting parties, secures the electronic transactions, indicates parties' consents and ensures the integrity of a document. In all the existing electronic signatures laws, electronic signatures have been recognised as equivalent to handwritten signatures. Certificate authorities (CAs), i.e. trusted third parties, can be licensed or unlicensed, public or private. The CA industry has not developed as expected since the 1990s because the private sector is 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. The mutual recognition of foreign certificates for electronic signatures is a prerequisite for the successful integration of e-business into the global economy. Thus the establishment of national, regional and international legislation 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. The employment of the 'functional equivalent' or 'technology-neutral' principle will be beneficial to the enhancement of cross-border recognition.

The fourth solution tackles the issue concerning 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 interactions and transactions. On the other hand, the free flow of data between different nations is necessary to stimulate international business transactions and globalisation. In the information society, legislation on data privacy protection shall be equipped to keep the balance between the free flow of data information and the fundamental human rights of privacy. Self-regulation in data privacy protection has also been encouraged by international legislative instruments; however, there should be procedures in law to examine whether

companies strictly comply with their privacy policies. Private trusted third-party services, such as the TRUSTe programme, can also provide supervision and enhance enforceability of data privacy protection in companies. Overall national, regional and international legislation shall include a four steps in common approach for data privacy protection:

- The first step is that service providers supervised by competent authorities should take appropriate technological and legislative measures to safeguard security.
- The second step is that service providers have a legal duty to inform users explicitly prior to obtaining their consent concerning the collection, process and storage of data.
- The third step is that service providers shall allow users to give and withdraw their consent freely as users have 'the right to be forgotten'.
- The fourth step is to enhance the implementation and enforcement of data privacy protection including notification of data breach without undue delay (i.e. within 24 hours) to competent authorities where feasible.

The fifth solution relates to the establishment of a mechanism that strikes a balance among different rights holders and ensures fairness of the liability of Internet service providers. The notice and takedown (NTD) system has become an effective measure to reduce the effects of illegal content (such as selling counterfeit goods or disclosing personal information) on websites. In the EU and US, if service providers act expeditiously to remove or to disable access to the information upon obtaining knowledge or awareness of illegal content, service providers should be exempted from liability,[9] though there is no consistent formality and timing regarding serving notice and counter-notice. According to research findings in this book, it is feasible to incorporate the 'online dispute resolution (ODR) mechanism' into the 'NTD system' and merge the 'NTD system' with the 'data breach notification mechanism', which can be considered a way forward to further promote the fairness and efficiency of consumer protection online.

The sixth solution focuses on the issue of determining jurisdiction and applicable law in electronic contracts. There are different jurisdictional rules in the EU, US and China, though the principles of party autonomy and general, special and exclusive jurisdictions are generally employed. The EU applies general and special jurisdiction according to the Brussels I Regulation, while 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

9 EC Directive on Electronic Commerce 2000, Article 14(1); and also Copyright Act Title 17 USC (1976), §512(g)(2)(c).

commercial characteristics. Chinese law is different from the EU and 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 the two main connecting 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, the 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/intangible goods with online delivery, 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.

As regards the determination of applicable law, the EU, US and China all distinguish the applicable law in cases of choice and in the absence of parties' choice. The principle of party autonomy, that parties are free to choose the governing law, is generally promoted, though interpreted and implemented differently in countries. In the absence of parties' choice, the principle of the seller's habitual residence has been considered a primary factor in the EU and China. If the principle of the seller's habitual residence cannot be applied, 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. Just like for the determination of Internet jurisdiction, tangible or digitised goods transacted online with physical delivery shall follow the same rules for the determination of the applicable law as in the offline world. The difference arises with contracts involving online delivery of digitised/intangible goods. According to the findings in the book, in this case, the seller's place of business (or habitual residence) is the most enduring connecting factor to B2B commercial contracts as it has an economic impact on its area, although this may lead to different results between the country where the law is chosen and the country where the court is located because a court in another country may have jurisdiction.

The seventh solution aims to clarify the mechanism of online dispute resolution (ODR) referring to electronic contracting disputes. ODR is a fairly new solution to the building of trust in electronic commercial transactions. Four successful examples – ICANN with WIPO – UDRP, eBay with SquareTrade, the 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, one of the six core principles of the conduct of ODR, is essential, since its success will encourage

electronic traders or businesses to use ODR to resolve their disputes. The outcomes of online mediation and negotiation should be able to be converted into binding and enforceable settlement agreements, while the decisions of online arbitration may constitute a valid arbitral award which is enforceable. Alternatively, the ODR service providers should have their self-enforcement or self-execution mechanisms to enforce contractual dispute settlements.

The eighth solution relates to the building of trusted e-commerce platforms to promote users' trust and confidence in online commercial activities. 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 matters of the validity of electronic contracts and incorporation of terms, the recognition of domestic and foreign certificates, electronic signatures and authentication, the technical and legal measures of data privacy protection, the establishment of an efficient NTD system with the 'data breach notification' mechanism, the determination of Internet jurisdiction and choice of law, as well as the deployment of appropriate principles and suitable procedures to online dispute resolution.

In short, 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 businesses. 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.

This page intentionally left blank

Appendices

This page intentionally left blank

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 sub-paragraph (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 organisations

1. A regional economic integration organisation 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 organisation shall in that case have the rights and obligations of a Contracting State, to the extent that that organisation has competence over matters governed by this Convention. Where the number of Contracting States is relevant in this Convention, the regional economic integration organisation shall not count as a Contracting State in addition to its member States that are Contracting States.

2. The regional economic integration organisation 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 organisation by its member States. The regional economic integration organisation 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 organisation where the context so requires.
4. This Convention shall not prevail over any conflicting rules of any regional economic integration organisation as applicable to parties whose respective places of business are located in States members of any such organisation, 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
Regulation (EU) No. 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No. 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR), OJ L 165/1, 18 June 2013

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee,[1]

Acting in accordance with the ordinary legislative procedure,[2]

Whereas:

(1) Article 169(1) and point (a) of Article 169(2) of the Treaty on the Functioning of the European Union (TFEU) provide that the Union is to contribute to the attainment of a high level of consumer protection through measures adopted pursuant to Article 114 TFEU. Article 38 of the Charter of Fundamental Rights of the European Union provides that Union policies are to ensure a high level of consumer protection.

1 OJ C181, 21 June 2012, p. 99.
2 Position of the European Parliament of 12 March 2013 (not yet published in the Official Journal) and Decision of the Council of 22 April 2013.

(2) In accordance with Article 26(2) TFEU, the internal market is to comprise an area without internal frontiers in which the free movement of goods and services is ensured. In order for consumers to have confidence in and benefit from the digital dimension of the internal market, it is necessary that they have access to simple, efficient, fast and low-cost ways of resolving disputes which arise from the sale of goods or the supply of services online. This is particularly important when consumers shop cross-border.

(3) In its Communication of 13 April 2011 entitled 'Single Market Act – Twelve levers to boost growth and strengthen confidence – "Working together to create new growth"', the Commission identified legislation on alternative dispute resolution (ADR) which includes an electronic commerce dimension as one of the twelve levers to boost growth and strengthen confidence in the Single Market.

(4) Fragmentation of the internal market impedes efforts to boost competitiveness and growth. Furthermore, the uneven availability, quality and awareness of simple, efficient, fast and low-cost means of resolving disputes arising from the sale of goods or provision of services across the Union constitutes a barrier within the internal market which undermines consumers' and traders' confidence in shopping and selling across borders.

(5) In its conclusions of 24–25 March and 23 October 2011, the European Council invited the European Parliament and the Council to adopt, by the end of 2012, a first set of priority measures to bring a new impetus to the Single Market.

(6) The internal market is a reality for consumers in their daily lives, when they travel, make purchases and make payments. Consumers are key players in the internal market and should therefore be at its heart. The digital dimension of the internal market is becoming vital for both consumers and traders. Consumers increasingly make purchases online and an increasing number of traders sell online. Consumers and traders should feel confident in carrying out transactions online so it is essential to dismantle existing barriers and to boost consumer confidence. The availability of reliable and efficient online dispute resolution (ODR) could greatly help achieve this goal.

(7) Being able to seek easy and low-cost dispute resolution can boost consumers' and traders' confidence in the digital Single Market. Consumers and traders, however, still face barriers to finding out-of-court solutions in particular to their disputes arising from cross-border online transactions. Thus, such disputes currently are often left unresolved.

(8) ODR offers a simple, efficient, fast and low-cost out-of- court solution to disputes arising from online transactions. However, there is currently a lack of mechanisms which allow consumers and traders to resolve such disputes through electronic means; this leads to consumer detriment, acts as a barrier, in particular, to cross-border online transactions, and creates an uneven playing field for traders, and thus hampers the overall development of online commerce.

(9) This Regulation should apply to the out-of-court resolution of disputes initiated by consumers resident in the Union against traders established in the Union which are covered by Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes (Directive on consumer ADR).[3]

(10) In order to ensure that the ODR platform can also be used for ADR procedures which allow traders to submit complaints against consumers, this Regulation should also apply to the out-of-court resolution of disputes initiated by traders against consumers where the relevant ADR procedures are offered by ADR entities listed in accordance with Article 20(2) of Directive 2013/11/EU. The application of this Regulation to such disputes should not impose any obligation on Member States to ensure that the ADR entities offer such procedures.

(11) Although in particular consumers and traders carrying out cross-border online transactions will benefit from the ODR platform, this Regulation should also apply to domestic online transactions in order to allow for a true level playing field in the area of online commerce.

(12) This Regulation should be without prejudice to 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.[4]

(13) The definition of 'consumer' should cover natural persons who are acting outside their trade, business, craft or profession. However, if the contract is concluded for purposes partly within and partly outside the person's trade (dual purpose contracts) and the trade purpose is so limited as not to be predominant in the overall context of the supply, that person should also be considered as a consumer.

(14) The definition of 'online sales or service contract' should cover a sales or service contract where the trader, or the trader's intermediary, has offered goods or services through a website or by other electronic means and the consumer has ordered those goods or services on that website or by other electronic means. This should also cover cases where the consumer has accessed the website or other information society service through a mobile electronic device such as a mobile telephone.

(15) This Regulation should not apply to disputes between consumers and traders that arise from sales or service contracts concluded offline and to disputes between traders.

(16) This Regulation should be considered in conjunction with Directive 2013/11/EU which requires Member States to ensure that all disputes between consumers resident and traders established in the Union which arise from the sale of goods or provisions of services can be submitted to an ADR entity.

3 See page 63 of this Official Journal.
4 OJ L136, 24 May 2008, p. 3.

(17) Before submitting their complaint to an ADR entity through the ODR platform, consumers should be encouraged by Member States to contact the trader by any appropriate means, with the aim of resolving the dispute amicably.

(18) This Regulation aims to create an ODR platform at Union level. The ODR platform should take the form of an interactive website offering a single point of entry to consumers and traders seeking to resolve disputes out-of-court which have arisen from online transactions. The ODR platform should provide general information regarding the out-of-court resolution of contractual disputes between traders and consumers arising from online sales and service contracts. It should allow consumers and traders to submit complaints by filling in an electronic complaint form available in all the official languages of the institutions of the Union and to attach relevant documents. It should transmit complaints to an ADR entity competent to deal with the dispute concerned. The ODR platform should offer, free of charge, an electronic case management tool which enables ADR entities to conduct the dispute resolution procedure with the parties through the ODR platform. ADR entities should not be obliged to use the case management tool.

(19) The Commission should be responsible for the development, operation and maintenance of the ODR platform and provide all technical facilities necessary for the functioning of the platform. The ODR platform should offer an electronic translation function which enables the parties and the ADR entity to have the information which is exchanged through the ODR platform and is necessary for the resolution of the dispute translated, where appropriate. That function should be capable of dealing with all necessary translations and should be supported by human intervention, if necessary. The Commission should also provide, on the ODR platform, information for complainants about the possibility of requesting assistance from the ODR contact points.

(20) The ODR platform should enable the secure interchange of data with ADR entities and respect the underlying principles of the European Interoperability Framework adopted pursuant to Decision 2004/387/EC of the European Parliament and of the Council of 21 April 2004 on interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC).[5]

(21) The ODR platform should be made accessible, in particular, through the 'Your Europe portal' established in accordance with Annex II to Decision 2004/387/EC, which provides access to pan-European, multilingual online information and interactive services to businesses and citizens in the Union. The ODR platform should be given prominence on the 'Your Europe portal'.

5 OJ L144, 30 April 2004, p. 62.

(22) An ODR platform at Union level should build on existing ADR entities in the Member States and respect the legal traditions of the Member States. ADR entities to which a complaint has been transmitted through the ODR platform should therefore apply their own procedural rules, including rules on cost. However, this Regulation intends to establish some common rules applicable to those procedures that will safeguard their effectiveness. This should include rules ensuring that such dispute resolution does not require the physical presence of the parties or their representatives before the ADR entity, unless its procedural rules provide for that possibility and the parties agree.

(23) Ensuring that all ADR entities listed in accordance with Article 20(2) of Directive 2013/11/EU are registered with the ODR platform should allow for full coverage in online out-of-court resolution for disputes arising from online sales or service contracts.

(24) This Regulation should not prevent the functioning of any existing dispute resolution entity operating online or of any ODR mechanism within the Union. It should not prevent dispute resolution entities or mechanisms from dealing with online disputes which have been submitted directly to them.

(25) ODR contact points hosting at least two ODR advisors should be designated in each Member State. The ODR contact points should support the parties involved in a dispute submitted through the ODR platform without being obliged to translate documents relating to that dispute. Member States should have the possibility to confer the responsibility for the ODR contact points on their centres of the European Consumer Centres Network. Member States should make use of that possibility in order to allow ODR contact points to fully benefit from the experience of the centres of the European Consumer Centres Network in facilitating the settlement of disputes between consumers and traders. The Commission should establish a network of ODR contact points to facilitate their cooperation and work and provide, in cooperation with Member States, appropriate training for ODR contact points.

(26) The right to an effective remedy and the right to a fair trial are fundamental rights laid down in Article 47 of the Charter of Fundamental Rights of the European Union. ODR is not intended to and cannot be designed to replace court procedures, nor should it deprive consumers or traders of their rights to seek redress before the courts. This Regulation should not, therefore, prevent parties from exercising their right of access to the judicial system.

(27) The processing of information under this Regulation should be subject to strict guarantees of confidentiality and should comply with the rules on the protection of personal data laid down in 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[6] and in Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.[7] Those rules should apply to the processing of personal data carried out under this Regulation by the various actors of the ODR platform, whether they act alone or jointly with other such actors.

(28) Data subjects should be informed about, and give their consent to, the processing of their personal data in the ODR platform, and should be informed about their rights with regard to that processing, by means of a comprehensive privacy notice to be made publicly available by the Commission and explaining, in clear and simple language, the processing operations performed under the responsibility of the various actors of the platform, in accordance with Articles 11 and 12 of Regulation (EC) No. 45/2001 and with national legislation adopted pursuant to Articles 10 and 11 of Directive 95/46/EC.

(29) This Regulation should be without prejudice to provisions on confidentiality in national legislation relating to ADR.

(30) In order to ensure broad consumer awareness of the existence of the ODR platform, traders established within the Union engaging in online sales or service contracts should provide, on their websites, an electronic link to the ODR platform. Traders should also provide their email address so that consumers have a first point of contact. A significant proportion of online sales and service contracts are concluded using online marketplaces, which bring together or facilitate online transactions between consumers and traders. Online marketplaces are online platforms which allow traders to make their products and services available to consumers. Such online marketplaces should therefore have the same obligation to provide an electronic link to the ODR platform. This obligation should be without prejudice to Article 13 of Directive 2013/11/EU concerning the requirement that traders inform consumers about the ADR procedures by which those traders are covered and about whether or not they commit to use ADR procedures to resolve disputes with consumers. Furthermore, that obligation should be without prejudice to point (t) of Article 6(1) and to Article 8 of Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights.[8] Point (t) of Article 6(1) of Directive 2011/83/EU stipulates for consumer contracts concluded at a distance or off premises, that the trader is to inform the consumer about the possibility of having recourse to an out-of-court complaint and redress mechanism to which

6 OJ L281, 23 November 1995, p. 31.
7 OJ L8, 12 January 2001, p. 1.
8 OJ L304, 22 November 2011, p. 64.

the trader is subject, and the methods for having access to it, before the consumer is bound by the contract. For the same consumer awareness reasons, Member States should encourage consumer associations and business associations to provide an electronic link to the website of the ODR platform.

(31) In order to take into account the criteria by which the ADR entities define their respective scopes of application the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission to adapt the information which a complainant is to provide in the electronic complaint form made available on the ODR platform. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.

(32) In order to ensure uniform conditions for the implementation of this Regulation implementing powers should be conferred on the Commission in respect of the functioning of the ODR platform, the modalities for the submission of a complaint and cooperation within the network of ODR contact points. Those powers should be exercised in accordance with Regulation (EU) No. 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers.[9] The advisory procedure should be used for the adoption of implementing acts relating to the electronic complaint form given its purely technical nature. The examination procedure should be used for the adoption of the rules concerning the modalities of cooperation between the ODR advisors of the network of ODR contact points.

(33) In the application of this Regulation, the Commission should consult, where appropriate, the European Data Protection Supervisor.

(34) Since the objective of this Regulation, namely to set up a European ODR platform for online disputes governed by common rules, cannot be sufficiently achieved by the Member States and can therefore, by reason of its scale and effects, be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(35) This Regulation respects fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union and specifically Articles 7, 8, 38 and 47 thereof.

9 OJ L55, 28 February 2011, p. 13.

(36) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No. 45/2001 and delivered an opinion on 12 January 2012,[10]

HAVE ADOPTED THIS REGULATION:

Chapter I General Provisions

Article 1 Subject matter

The purpose of this Regulation is, through the achievement of a high level of consumer protection, to contribute to the proper functioning of the internal market, and in particular of its digital dimension by providing a European ODR platform ('ODR platform') facilitating the independent, impartial, transparent, effective, fast and fair out-of-court resolution of disputes between consumers and traders online.

Article 2 Scope

1. This Regulation shall apply to the out-of-court resolution of disputes concerning contractual obligations stemming from online sales or service contracts between a consumer resident in the Union and a trader established in the Union through the intervention of an ADR entity listed in accordance with Article 20(2) of Directive 2013/11/EU and which involves the use of the ODR platform.
2. This Regulation shall apply to the out-of-court resolution of disputes referred to in paragraph 1, which are initiated by a trader against a consumer, in so far as the legislation of the Member State where the consumer is habitually resident allows for such disputes to be resolved through the intervention of an ADR entity.
3. Member States shall inform the Commission about whether or not their legislation allows for disputes referred to in paragraph 1, which are initiated by a trader against a consumer, to be resolved through the intervention of an ADR entity. Competent authorities shall, when they notify the list referred to in Article 20(2) of Directive 2013/11/EU, inform the Commission about which ADR entities deal with such disputes.
4. The application of this Regulation to disputes referred to in paragraph 1, which are initiated by a trader against a consumer, shall not impose any obligation on Member States to ensure that ADR entities offer procedures for the out-of-court resolution of such disputes.

10 OJ C136, 11 May 2012, p. 1.

Article 3 Relationship with other Union legal acts

This Regulation shall be without prejudice to Directive 2008/52/EC.

Article 4 Definitions

1. For the purposes of this Regulation:
   (a) 'consumer' means a consumer as defined in point (a) of Article 4(1) of Directive 2013/11/EU;
   (b) 'trader' means a trader as defined in point (b) of Article 4(1) of Directive 2013/11/EU;
   (c) 'sales contract' means a sales contract as defined in point (c) of Article 4(1) of Directive 2013/11/EU;
   (d) 'service contract' means a service contract as defined in point (d) of Article 4(1) of Directive 2013/11/EU;
   (e) 'online sales or service contract' means a sales or service contract where the trader, or the trader's intermediary, has offered goods or services on a website or by other electronic means and the consumer has ordered such goods or services on that website or by other electronic means;
   (f) 'online marketplace' means a service provider, as defined in point (b) of Article 2 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'),[11] which allows consumers and traders to conclude online sales and service contracts on the online marketplace's website;
   (g) 'electronic means' means electronic equipment for the processing (including digital compression) and storage of data which is entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means;
   (h) 'alternative dispute resolution procedure' ('ADR procedure') means a procedure for the out-of-court resolution of disputes as referred to in Article 2 of this Regulation;
   (i) 'alternative dispute resolution entity' ('ADR entity') means an ADR entity as defined in point (h) of Article 4(1) of Directive 2013/11/EU;
   (j) 'complainant party' means the consumer who or the trader that has submitted a complaint through the ODR platform;
   (k) 'respondent party' means the consumer against whom or the trader against whom a complaint has been submitted through the ODR platform;

11 OJ L178, 17 July 2000, p. 1.

(l) 'competent authority' means a public authority as defined in point (i) of Article 4(1) of Directive 2013/11/EU;
(m) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an 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 that person's physical, physiological, mental, economic, cultural or social identity.

2. The place of establishment of the trader and of the ADR entity shall be determined in accordance with Article 4(2) and (3) of Directive 2013/11/EU, respectively.

Chapter II ODR Platform

Article 5 Establishment of the ODR platform

1. The Commission shall develop the ODR platform and be responsible for its operation, including all the translation functions necessary for the purpose of this Regulation, its maintenance, funding and data security. The ODR platform shall be user-friendly. The development, operation and maintenance of the ODR platform shall ensure that the privacy of its users is respected from the design stage ('privacy by design') and that the ODR platform is accessible and usable by all, including vulnerable users ('design for all'), as far as possible.
2. The ODR platform shall be a single point of entry for consumers and traders seeking the out-of-court resolution of disputes covered by this Regulation. It shall be an interactive website which can be accessed electronically and free of charge in all the official languages of the institutions of the Union.
3. The Commission shall make the ODR platform accessible, as appropriate, through its websites which provide information to citizens and businesses in the Union and, in particular, through the 'Your Europe portal' established in accordance with Decision 2004/387/EC.
4. The ODR platform shall have the following functions:
   (a) to provide an electronic complaint form which can be filled in by the complainant party in accordance with Article 8;
   (b) to inform the respondent party about the complaint;
   (c) to identify the competent ADR entity or entities and transmit the complaint to the ADR entity, which the parties have agreed to use, in accordance with Article 9;
   (d) to offer an electronic case management tool free of charge, which enables the parties and the ADR entity to conduct the dispute resolution procedure online through the ODR platform;
   (e) to provide the parties and ADR entity with the translation of information which is necessary for the resolution of the dispute and is exchanged through the ODR platform;

(f) to provide an electronic form by means of which ADR entities shall transmit the information referred to in point (c) of Article 10;
(g) to provide a feedback system which allows the parties to express their views on the functioning of the ODR platform and on the ADR entity which has handled their dispute;
(h) to make publicly available the following:
  (i) general information on ADR as a means of out-of-court dispute resolution;
  (ii) information on ADR entities listed in accordance with Article 20(2) of Directive 2013/11/EU which are competent to deal with disputes covered by this Regulation;
  (iii) an online guide about how to submit complaints through the ODR platform;
  (iv) information, including contact details, on ODR contact points designated by the Member States in accordance with Article 7(1) of this Regulation;
  (v) statistical data on the outcome of the disputes which were transmitted to ADR entities through the ODR platform.

5. The Commission shall ensure that the information referred to in point (h) of paragraph 4 is accurate, up to date and provided in a clear, understandable and easily accessible way.
6. ADR entities listed in accordance with Article 20(2) of Directive 2013/11/EU which are competent to deal with disputes covered by this Regulation shall be registered electronically with the ODR platform.
7. The Commission shall adopt measures concerning the modalities for the exercise of the functions provided for in paragraph 4 of this Article through implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 16(3) of this Regulation.

Article 6 Testing of the ODR platform

1. The Commission shall, by 9 January 2015, test the technical functionality and user-friendliness of the ODR platform and of the complaint form, including with regard to translation. The testing shall be carried out and evaluated in cooperation with experts in ODR from the Member States and consumer and trader representatives. The Commission shall submit a report to the European Parliament and the Council of the result of the testing and take the appropriate measures to address potential problems in order to ensure the effective functioning of the ODR platform.
2. In the report referred to in paragraph 1 of this Article, the Commission shall also describe the technical and organisational measures it intends to take to ensure that the ODR platform meets the privacy requirements set out in Regulation (EC) No. 45/2001.

Article 7 Network of ODR contact points

1. Each Member State shall designate one ODR contact point and communicate its name and contact details to the Commission. The Member States may confer responsibility for the ODR contact points on their centres of the European Consumer Centres Network, on consumer associations or on any other body. Each ODR contact point shall host at least two ODR advisors.
2. The ODR contact points shall provide support to the resolution of disputes relating to complaints submitted through the ODR platform by fulfilling the following functions:
   (a) if requested, facilitating communication between the parties and the competent ADR entity, which may include, in particular:
      (i) assisting with the submission of the complaint and, where appropriate, relevant documentation;
      (ii) providing the parties and ADR entities with general information on consumer rights in relation to sales and service contracts which apply in the Member State of the ODR contact point which hosts the ODR advisor concerned;
      (iii) providing information on the functioning of the ODR platform;
      (iv) providing the parties with explanations on the procedural rules applied by the ADR entities identified;
      (v) informing the complainant party of other means of redress when a dispute cannot be resolved through the ODR platform;
   (b) submitting, based on the practical experience gained from the performance of their functions, every two years an activity report to the Commission and to the Member States.
3. The ODR contact point shall not be obliged to perform the functions listed in paragraph 2 in the case of disputes where the parties are habitually resident in the same Member State.
4. Notwithstanding paragraph 3, the Member States may decide, taking into account national circumstances, that the ODR contact point performs one or more functions listed in paragraph 2 in the case of disputes where the parties are habitually resident in the same Member State.
5. The Commission shall establish a network of contact points ('ODR contact points network') which shall enable cooperation between contact points and contribute to the performance of the functions listed in paragraph 2.
6. The Commission shall at least twice a year convene a meeting of members of the ODR contact points network in order to permit an exchange of best practice, and a discussion of any recurring problems encountered in the operation of the ODR platform.
7. The Commission shall adopt the rules concerning the modalities of the cooperation between the ODR contact points through implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 16(3).

Article 8 Submission of a complaint

1. In order to submit a complaint to the ODR platform the complainant party shall fill in the electronic complaint form. The complaint form shall be user-friendly and easily accessible on the ODR platform.
2. The information to be submitted by the complainant party shall be sufficient to determine the competent ADR entity. That information is listed in the Annex to this Regulation. The complainant party may attach documents in support of the complaint.
3. In order to take into account the criteria by which the ADR entities, that are listed in accordance with Article 20(2) of Directive 2013/11/EU and that deal with disputes covered by this Regulation, define their respective scopes of application, the Commission shall be empowered to adopt delegated acts in accordance with Article 17 of this Regulation to adapt the information listed in the Annex to this Regulation.
4. The Commission shall lay down the rules concerning the modalities for the electronic complaint form by means of implementing acts. Those implementing acts shall be adopted in accordance with the advisory procedure referred to in Article 16(2).
5. Only data which are accurate, relevant and not excessive in relation to the purposes for which they are collected shall be processed through the electronic complaint form and its attachments.

Article 9 Processing and transmission of a complaint

1. A complaint submitted to the ODR platform shall be processed if all the necessary sections of the electronic complaint form have been completed.
2. If the complaint form has not been fully completed, the complainant party shall be informed that the complaint cannot be processed further, unless the missing information is provided.
3. Upon receipt of a fully completed complaint form, the ODR platform shall, in an easily understandable way and without delay, transmit to the respondent party, in one of the official languages of the institutions of the Union chosen by that party, the complaint together with the following data:
   (a) information that the parties have to agree on an ADR entity in order for the complaint to be transmitted to it, and that, if no agreement is reached by the parties or no competent ADR entity is identified, the complaint will not be processed further;
   (b) information about the ADR entity or entities which are competent to deal with the complaint, if any are referred to in the electronic complaint form or are identified by the ODR platform on the basis of the information provided in that form;

(c) in the event that the respondent party is a trader, an invitation to state within 10 calendar days:
   – whether the trader commits to, or is obliged to use, a specific ADR entity to resolve disputes with consumers, and
   – unless the trader is obliged to use a specific ADR entity, whether the trader is willing to use any ADR entity or entities from those referred to in point (b);

(d) in the event that the respondent party is a consumer and the trader is obliged to use a specific ADR entity, an invitation to agree within 10 calendar days on that ADR entity or, in the event that the trader is not obliged to use a specific ADR entity, an invitation to select one or more ADR entities from those referred to in point (b);

(e) the name and contact details of the ODR contact point in the Member State where the respondent party is established or resident, as well as a brief description of the functions referred to in point (a) of Article 7(2).

4. Upon receipt from the respondent party of the information referred to in point (c) or point (d) of paragraph 3, the ODR platform shall in an easily understandable way and without delay communicate to the complainant party, in one of the official languages of the institutions of the Union chosen by that party, the following information:

(a) the information referred to in point (a) of paragraph 3;

(b) in the event that the complainant party is a consumer, the information about the ADR entity or entities stated by the trader in accordance with point (c) of paragraph 3 and an invitation to agree within 10 calendar days on an ADR entity;

(c) in the event that the complainant party is a trader and the trader is not obliged to use a specific ADR entity, the information about the ADR entity or entities stated by the consumer in accordance with point (d) of paragraph 3 and an invitation to agree within 10 calendar days on an ADR entity;

(d) the name and contact details of the ODR contact point in the Member State where the complainant party is established or resident, as well as a brief description of the functions referred to in point (a) of Article 7(2).

5. The information referred to in point (b) of paragraph 3 and in points (b) and (c) of paragraph 4 shall include a description of the following characteristics of each ADR entity:

(a) the name, contact details and website address of the ADR entity;

(b) the fees for the ADR procedure, if applicable;

(c) the language or languages in which the ADR procedure can be conducted;

(d) the average length of the ADR procedure;

(e) the binding or non-binding nature of the outcome of the ADR procedure;

(f) the grounds on which the ADR entity may refuse to deal with a given dispute in accordance with Article 5(4) of Directive 2013/11/EU.

6. The ODR platform shall automatically and without delay transmit the complaint to the ADR entity that the parties have agreed to use in accordance with paragraphs 3 and 4.
7. The ADR entity to which the complaint has been transmitted shall without delay inform the parties about whether it agrees or refuses to deal with the dispute in accordance with Article 5(4) of Directive 2013/11/EU. The ADR entity which has agreed to deal with the dispute shall also inform the parties of its procedural rules and, if applicable, of the costs of the dispute resolution procedure concerned.
8. Where the parties fail to agree within 30 calendar days after submission of the complaint form on an ADR entity, or the ADR entity refuses to deal with the dispute, the complaint shall not be processed further. The complainant party shall be informed of the possibility of contacting an ODR advisor for general information on other means of redress.

Article 10 Resolution of the dispute

An ADR entity which has agreed to deal with a dispute in accordance with Article 9 of this Regulation shall:

(a) conclude the ADR procedure within the deadline referred to in point (e) of Article 8 of Directive 2013/11/EU;
(b) not require the physical presence of the parties or their representatives, unless its procedural rules provide for that possibility and the parties agree;
(c) without delay transmit the following information to the ODR platform:
  (i) the date of receipt of the complaint file;
  (ii) the subject-matter of the dispute;
  (iii) the date of conclusion of the ADR procedure;
  (iv) the result of the ADR procedure;
(d) not be required to conduct the ADR procedure through the ODR platform.

Article 11 Database

The Commission shall take the necessary measures to establish and maintain an electronic database in which it shall store the information processed in accordance with Article 5(4) and point (c) of Article 10 taking due account of Article 13(2).

Article 12 Processing of personal data

1. Access to information, including personal data, related to a dispute and stored in the database referred to in Article 11 shall be granted, for the

purposes referred to in Article 10, only to the ADR entity to which the dispute was transmitted in accordance with Article 9. Access to the same information shall be granted also to ODR contact points, in so far as it is necessary, for the purposes referred to in Article 7(2) and (4).

2. The Commission shall have access to information processed in accordance with Article 10 for the purposes of monitoring the use and functioning of the ODR platform and drawing up the reports referred to in Article 21. It shall process personal data of the users of the ODR platform in so far as it is necessary for the operation and maintenance of the ODR platform, including for the purposes of monitoring the use of the ODR platform by ADR entities and ODR contact points.
3. Personal data related to a dispute shall be kept in the database referred to in paragraph 1 of this Article only for the time necessary to achieve the purposes for which they were collected and to ensure that data subjects are able to access their personal data in order to exercise their rights, and shall be automatically deleted, at the latest, six months after the date of conclusion of the dispute which has been transmitted to the ODR platform in accordance with point (iii) of point (c) of Article 10. That retention period shall also apply to personal data kept in national files by the ADR entity or the ODR contact point which dealt with the dispute concerned, except if the procedural rules applied by the ADR entity or any specific provisions of national law provide for a longer retention period.
4. Each ODR advisor shall be regarded as a controller with respect to its data processing activities under this Regulation, in accordance with point (d) of Article 2 of Directive 95/46/EC, and shall ensure that those activities comply with national legislation adopted pursuant to Directive 95/46/EC in the Member State of the ODR contact point hosting the ODR advisor.
5. Each ADR entity shall be regarded as a controller with respect to its data processing activities under this Regulation, in accordance with point (d) of Article 2 of Directive 95/46/EC, and shall ensure that those activities comply with national legislation adopted pursuant to Directive 95/46/EC in the Member State where the ADR entity is established.
6. In relation to its responsibilities under this Regulation and the processing of personal data involved therein, the Commission shall be regarded as a controller in accordance with point (d) of Article 2 of Regulation (EC) No. 45/2001.

Article 13 Data confidentiality and security

1. ODR contact points shall be subject to rules of professional secrecy or other equivalent duties of confidentiality laid down in the legislation of the Member State concerned.

2. The Commission shall take the appropriate technical and organisational measures to ensure the security of information processed under this Regulation, including appropriate data access control, a security plan and a security incident management, in accordance with Article 22 of Regulation (EC) No. 45/2001.

Article 14 Consumer information

1. Traders established within the Union engaging in online sales or service contracts, and online marketplaces established within the Union, shall provide on their websites an electronic link to the ODR platform. That link shall be easily accessible for consumers. Traders established within the Union engaging in online sales or service contracts shall also state their e-mail addresses.
2. Traders established within the Union engaging in online sales or service contracts, which are committed or obliged to use one or more ADR entities to resolve disputes with consumers, shall inform consumers about the existence of the ODR platform and the possibility of using the ODR platform for resolving their disputes. They shall provide an electronic link to the ODR platform on their websites and, if the offer is made by e-mail, in that e-mail. The information shall also be provided, where applicable, in the general terms and conditions applicable to online sales and service contracts.
3. Paragraphs 1 and 2 of this Article shall be without prejudice to Article 13 of Directive 2013/11/EU and the provisions on consumer information on out-of-court redress procedures contained in other Union legal acts, which shall apply in addition to this Article.
4. The list of ADR entities referred to in Article 20(4) of Directive 2013/11/EU and its updates shall be published in the ODR platform.
5. Member States shall ensure that ADR entities, the centres of the European Consumer Centres Network, the competent authorities defined in Article 18(1) of Directive 2013/11/EU, and, where appropriate, the bodies designated in accordance with Article 14(2) of Directive 2013/11/EU provide an electronic link to the ODR platform.
6. Member States shall encourage consumer associations and business associations to provide an electronic link to the ODR platform.
7. When traders are obliged to provide information in accordance with paragraphs 1 and 2 and with the provisions referred to in paragraph 3, they shall, where possible, provide that information together.

Article 15 Role of the competent authorities

The competent authority of each Member State shall assess whether the ADR entities established in that Member State comply with the obligations set out in this Regulation.

Chapter III Final Provisions

Article 16 Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No. 182/2011.
2. Where reference is made to this paragraph, Article 4 of Regulation (EU) No. 182/2011 shall apply.
3. Where reference is made to this paragraph, Article 5 of Regulation (EU) No. 182/2011 shall apply.
4. Where the opinion of the committee under paragraphs 2 and 3 is to be obtained by written procedure, that procedure shall be terminated without result when, within the time-limit for delivery of the opinion, the chair of the committee so decides or a simple majority of committee members so request.

Article 17 Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.
2. The power to adopt delegated acts referred to in Article 8(3) shall be conferred for an indeterminate period of time from 8 July 2013.
3. The delegation of power referred to in Article 8(3) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.
4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.
5. A delegated act adopted pursuant to Article 8(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.

Article 18 Penalties

Member States shall lay down the rules on penalties applicable to infringements of this Regulation and shall take all measures necessary to ensure that

they are implemented. The penalties provided for must be effective, proportionate and dissuasive.

Article 19 Amendment to Regulation (EC) No. 2006/2004

In the Annex to Regulation (EC) No. 2006/2004 of the European Parliament and of the Council[12] the following point is added:

> '21. Regulation (EU) No. 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes (Regulation on consumer ODR) (OJ L 165, 18.6.2013, p. 1): Article 14.'

Article 20 Amendment to Directive 2009/22/EC

Directive 2009/22/EC of the European Parliament and of the Council[13] is amended as follows:

(1) in Article 1(1) and (2) and point (b) of Article 6(2), the words 'Directives listed in Annex I' are replaced with the words 'Union acts listed in Annex I';
(2) in the heading of Annex I, the words 'LIST OF DIRECTIVES' are replaced by the words 'LIST OF UNION ACTS';
(3) in Annex I, the following point is added:

'15. Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes (Regulation on consumer ODR) (OJ L 165, 18.6.2013, p. 1): Article 14.'

Article 21 Reports

1. The Commission shall report to the European Parliament and the Council on the functioning of the ODR platform on a yearly basis and for the first time one year after the ODR platform has become operational.
2. By 9 July 2018 and every three years thereafter the Commission shall submit to the European Parliament and the Council a report on the application of this Regulation, including in particular on the user-friendliness of the complaint form and the possible need for adaptation of the information listed in the Annex to this Regulation. That report shall be accompanied, if necessary, by proposals for adaptations to this Regulation.
3. Where the reports referred to in paragraphs 1 and 2 are to be submitted in the same year, only one joint report shall be submitted.

12 OJ L364, 9 December 2004, p. 1.
13 OJ L110, 1 May 2009, p. 30.

Article 22 Entry into force

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.
2. This Regulation shall apply from 9 January 2016, except for the following provisions:
   - Article 2(3) and Article 7(1) and (5), which shall apply from 9 July 2015,
   - Article 5(1) and (7), Article 6, Article 7(7), Article 8(3) and (4) and Articles 11, 16 and 17, which shall apply from 8 July 2013.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Strasbourg, 21 May 2013.

Appendix 3
Law of People's Republic of China on the Laws Applicable to Foreign-related Civil Relations 2010

Decree of the President of the People's Republic of China No. 36 (Adopted at the 17th session of the Standing Committee of the 11th National People's Congress, 28 October 2010)

It is hereby promulgated that the Law of the People's Republic of China on the Laws Applicable to Foreign-related Civil Relations has been adopted on 28 October 2010 at the 17th session of the Standing Committee of the 11th National People's Congress of the People's Republic of China, which will come into effect as from 1 April 2011.

HU Jintao, President of the People's Republic of China
28 October 2010

Content

Chapter One General Provisions

ARTICLE 1 This law is formulated with a view to specifying the laws applicable to foreign-related civil relations, resolving foreign-related civil disputes fairly and safeguarding the legitimate rights and interests of the parties.

ARTICLE 2 The laws applicable to foreign-related civil relations shall be specified in accordance with this law. Where other statutes have a special and different provision on the law applicable to a foreign-related civil relation, that provision shall be followed.

Where no applicable law to a foreign-related civil relation has been specified in this law or other statutes, the law that is most closely connected with the foreign-related civil relation shall be applied.

ARTICLE 3 The parties may explicitly choose the law applicable to their foreign-related civil relation in accordance with the provisions of this law.

ARTICLE 4 Where a mandatory provision of the law of the People's Republic of China ('PRC') exists with respect to a foreign-related civil relation, that mandatory provision shall be applied directly.

ARTICLE 5 Where the application of a foreign law will be prejudicial to the social and public interest of the PRC, the PRC law shall be applied.

ARTICLE 6 Where a foreign law is applicable to a foreign-related civil relation and different laws are implemented in the different regions of that country, the law of the region that is most closely connected with the foreign-related civil relation shall be applied.

ARTICLE 7 Limitation period is governed by the law that should be applicable to the foreign-related civil relation.

ARTICLE 8 Classification of foreign-related civil relations is governed by the law of the forum.

ARTICLE 9 The foreign law applicable to a foreign-related civil relation does not include the conflict rules of that country.

ARTICLE 10 The foreign law applicable to a foreign-related civil relation will be ascertained by the relevant people's court, arbitration institution or the administrative agency. Where the parties have chosen a foreign law to be applicable, they shall adduce the law of that country.

Where the foreign law cannot be ascertained or the law of that country does not have a relevant provision, the PRC law shall be applied.

Chapter Two Civil Entities

ARTICLE 11 Civil capacity of a natural person is governed by the law of the place where the person habitually resides.

ARTICLE 12 Civil competence of a natural person is governed by the law of the place where the person habitually resides.

Where a natural person engaging in civil activities is deemed incompetent pursuant to the law of the place where the person habitually resides but competent according to the law of the place where the act is performed, the law of the place where the act is performed shall be applied, with the exception of those related to marriage, family or succession.

ARTICLE 13 Declaration of missing or declaration of death are governed by the law of the place where the natural person habitually resides.

ARTICLE 14 Items such as the civil capacity, civil competence, organisational structure and shareholder rights, etc. of a juridical person and its branches are governed by the law of the place of registration.

The law of the principal place of business of a juridical person may be applicable where such principal place of business is different from the place of registration. The principal place of business of a juridical person shall be deemed to be its habitual residence.

ARTICLE 15 The content of personality right is governed by the law of the obligee's habitual residence.

ARTICLE 16 Agency is governed by the law of the place where the act of agency occurs. However, the civil relation between the principal and agent will be governed by the law of the place where the agency relationship is established.

The parties may by agreement choose the law applicable to their relation of commissioned agency.

ARTICLE 17 The parties may by agreement choose the law applicable to trust. Absent any choice by the parties, the law of the place where the trust asset locates or where the trust relation is established shall be applied.

ARTICLE 18 The parties may by agreement choose the law applicable to their arbitration agreement. Absent any choice by the parties, the law of the place where the arbitration institution locates or the law of the seat of arbitration shall be applied.

ARTICLE 19 Where national law is applicable pursuant to this law and a natural person has dual or multiple nationalities, the national law of the country where the natural person has his/her habitual residence shall be applied. Where no habitual residence can be found in any country of his/her nationalities, the national law of the country with which he/she is most closely connected shall be applied. Where a natural person is stateless or his/her nationality is unknown, the law of his/her habitual residence shall be applied.

ARTICLE 20 Where the law of the habitual residence is applicable pursuant to this law and a natural person's habitual residence cannot be ascertained, the law of his/her present residence shall be applied.

Chapter Three Marriage and Family

ARTICLE 21 Conditions of marriage are governed by the law of the parties' common habitual residence. Absent common habitual residence, the law of their common nationality shall be applied. Absent common nationality, the law of the place where the marriage is concluded shall be applied, if the marriage is concluded in a party's habitual residence or in the country of a party's nationality.

ARTICLE 22 Formalities of marriage are valid if they conform to the law of the place where the marriage is concluded, or the law of a party's habitual residence or nationality.

ARTICLE 23 Personal relation of spouses is governed by the law of their common habitual residence. Absent common habitual residence, the law of their common nationality shall be applied.

ARTICLE 24 In respect of spousal property, the parties may by agreement choose to apply the law of a party's habitual residence or nationality, or the law of the place where the main property locates. Absent any choice by the parties, the law of their common habitual residence shall be applied; absent common habitual residence, the law of their common nationality shall be applied.

ARTICLE 25 Personal and property relations between parents and children are governed by the law of their common habitual residence. Absent common habitual residence, the law of a party's habitual residence or nationality, which better protects the rights and interests of the weaker party, shall be applied.

ARTICLE 26 In respect of consented divorce, the parties may by agreement choose to apply the law of a party's habitual residence or nationality. Absent any choice by the parties, the law of their common habitual residence shall be applied; absent common habitual residence, the law of their common nationality shall be applied; absent common nationality, the law of the place where the agency responsible for completing the divorce formalities locates shall be applied.

ARTICLE 27 Divorce decided by a court is governed by the law of the forum.

ARTICLE 28 Conditions and formalities of adoption are governed by the laws of the habitual residence of the adopter and the adoptee. The effect of adoption is governed by the law of the adopter's habitual residence when the adoption occurs. The termination of adoption relation is governed by the law of the adoptee's habitual residence when the adoption occurs or by the law of the forum.

ARTICLE 29 Support[1] is governed by the law of a party's habitual residence, or the law of a party's nationality, or the law of the place where the main property locates, which better protects the rights and interests of the person being supported.

1 The concept of 'support' used herein embraces marital maintenance and support of a minor or elderly dependent.

ARTICLE 30 Guardianship is governed by the law of a party's habitual residence or nationality, which better protects the rights and interests of the person under custody.

Chapter Four Succession

ARTICLE 31 Statutory succession is governed by the law of the habitual residence of the deceased when he/she dies. However, statutory succession of immovable property is governed by the law where the immovable property locates.

ARTICLE 32 A will is considered formed if the testamentary form conforms to the law of the habitual residence of the testator when he/she creates the will or when he/she dies, or to the law of his/her nationality, or to the law of the place where the act of creating the will occurs.

ARTICLE 33 The effect of a will is governed by the habitual residence of the deceased when he/she creates the will or when he/she dies, or by the law of his/her nationality.

ARTICLE 34 Matters of estate administration, etc. are governed by the law of the place where the estate locates.

ARTICLE 35 Ownership of estate without a successor is governed by the law of the place where the estate locates when the deceased dies.

Chapter Five Rights in rem

ARTICLE 36 Rights in rem in immovable property is governed by the law of the place where the immovable property locates.

ARTICLE 37 The parties may by agreement choose the law applicable to rights in rem in movable property. Absent any choice by the parties, the law of the place where the property locates when the legal fact occurs shall be applied.

ARTICLE 38 The parties may by agreement choose the law applicable to the change of the rights in rem in movable property which is in transit. Absent any choice by the parties, the law of the destination of transportation shall be applied.

ARTICLE 39 Valuable papers are governed by the law of the place where the rights in a valuable paper are realised or by another law which is most closely connected to such valuable paper.

ARTICLE 40 Pledge of a right is governed by the law of the place where such pledge is created.

Chapter Six Obligations

ARTICLE 41 The parties may by agreement choose the law applicable to their contract. Absent any choice by the parties, the law of the habitual residence of a party whose performance of obligation is most characteristic of the contract or the law that most closely connected with the contract shall be applied.

ARTICLE 42 A consumer contract is governed by the law of the consumer's habitual residence. Where the consumer chooses the law of the place where the commodity or the service is provided, or where the business operator does not engage in any business activity in the habitual residence of the consumer, the law of the place where the commodity or service is provided shall be applied.

ARTICLE 43 An employment contract is governed by the law of the place where the employee works. Where the working place of the employee cannot be ascertained, the law of the principal place of business of the employer shall be applied. Labour service placement may be governed by the law of the place where the service placement is arranged.

ARTICLE 44 Tortious liability is governed by the law of the place of tortious act. Where the parties have common habitual residence, the law of their common habitual residence shall be applied. Where the parties have chosen by agreement an applicable law after the tortious act occurs, the agreement shall be followed.

ARTICLE 45 Product liability is governed by the law of the habitual residence of the victim. Where the victim chooses the law of the principal place of business of the tortfeasor or the law where the damage occurs, or the tortfeasor does not engage in any business activity in the victim's habitual residence, the law of the tortfeasor's principal place of business or the place where the damage occurs shall be applied.

ARTICLE 46 Infringement via Internet or by other means of personality rights such as right to name, right to image, right of reputation and privacy right are governed by the law of the habitual residence of the victim.

ARTICLE 47 Unjust enrichment and *Negotiorum gestio* are governed by the law chosen by the parties by agreement. Absent any choice by the parties, the law of their common habitual residence shall be applied. Absent common habitual residence, the law of the place where the unjust enrichment or *Negotiorum gestio* occurs shall be applied.

Chapter Seven Intellectual Property Rights

ARTICLE 48 Proprietorship and content of intellectual property rights are governed by the law of the place where protection is sought.

ARTICLE 49 The parties may by agreement choose the law applicable to the transfer and license of intellectual property rights. Absent any choice by the parties, the relevant provisions of this law on contract are applicable.

ARTICLE 50 Liability for infringing intellectual property rights is governed by the law of the place where protection is sought. The parties may also choose to apply the law of the forum after the infringement occurs.

Chapter Eight Miscellaneous Provisions

ARTICLE 51 Where Article 146, Article 147 of the General Principles of Civil Law of the PRC and Article 36 of the Succession Law of the PRC are inconsistent with the provisions of this law, this law shall prevail.

ARTICLE 52 This law shall take effect as from 1 April 2011.

This translation is available at http://www.wipo.int/wipolex/en/details.jsp?id=8423 (last accessed 30 June 2013).

Index

Added to a page number 'n' denotes notes.