Technical Assistance Consultants' Draft Report

DRAFT REPORT

Project Number: TA6618

Date: 1 January 2023

Mongolia: Enabling a conducive environment for e-commerce

OUTPUT 1: Legal and regulatory barriers to effective and efficient e-commerce identified and recommendations for improvement developed.

Prepared by:

- John D. Gregory – International Consultant, Canada
- Delgermaa Anbat – National Consultant, Mongolia

Beneficiary:

- Ministry of Digital Development and Communications, Mongolia

Asian Development Bank

Project Number: TA6618

Date: 1 January 2023

The Consultants

John Gregory *(international)* is a commercial and technology lawyer in Ontario, Canada, who developed legislation for the provincial government for over 30 years. He was a leading Canadian expert on laws relating to electronic communications, as well as serving on the Canadian delegation to the United Nations (UN) Commission on International Trade Law (CITRAL) Working Group on Electronic Commerce for 16 years. Since his retirement from the government in 2016, he has been active as a consultant in this field, notably for Asian clients like UN Economic and Social Commission for Asia and the Pacific (ESCAP), the Central Asia Regional Economic Cooperation (CAREC) Program Institute and the ADB.

Delgermaa Anbat (*national*) is a Licensed Lawyer and Attorney-at-Law and Managing Partner at Mongolian Legal Experts LLP. She has about 20 years of professional experience as Legal Advisor, Legal Researcher, and Lawyer through consultancy work both for the national and international levels. She has extensive experience in legislative and research projects for different ministries of the Government of Mongolia and for the Asian Development Bank. She has participated in drafting several laws and regulations on technical, financial and legal topics.

ADB PROJECT ON MONGOLIA

SECOND MILESTONE: DRAFT REPORT

John D. Gregory with Anbat Delgermaa

DRAFT *1 January 2023*

Contents

c. UN/ESCSAP Framework Agreement on Facilitation of Cross-Border Paperless Trade in Asia and the Pacific
d. Mongolia-Japan Free Trade Agreement

2. Potential trade agreements for Mongolia
a. Regional Comprehensive Economic Partnership (RCEP)

B. Regional economic cooperation agreements
1. Now in force in Mongolia
a. Central Asia Regional Economic Cooperation (CAREC)

C. Instruments that expressly target e-commerce for its own sake

1. E-Commerce instruments now in force in Mongolia
a. United Nations Convention on the Use of Electronic Communications in International Contracts (the E-Communications Convention)
b. Customs Convention on the International Transport of Goods under Cover of TIR Carnets (TIR Convention)

2. Potential instruments on electronic communications

a. WTO Joint Statement Initiative on e-Commerce

b. UNCITRAL Model Laws on Electronic Commerce and Electronic Signatures

c. UNCITRAL Model Law on Electronic Transferable Records

D. Other current treaties and related agreements
1. Treaties now in force in Mongolia
a. Convention on the International Sale of Goods (CISG)
b. Sanitary and Phytosanitary (SPS) Agreement
c. Convention on Trade in Endangered Species (CITES)
d. UN Convention on the Harmonization of Frontier Controls of Goods
e. United Nations Layout Key for Trade Documents

E. International standards
1. Now available
a. UN Centre for Trade Facilitation (CEFACT) recommendations
b. International Standards Organization (ISO) standards
c. Internet Standards

V. FRAMEWORK AND CONTEXT FOR ELECTRONIC COMMERCE
Principles of Regulation

A. A Law on electronic commerce
B. An e-commerce business
1. International perspectives
a. Defining an e-commerce business
b. Regulating e-commerce businesses
c. “The State of the Art”
2. Trading platforms

Regulating other areas of e-commerce

C. Consumer protection
   Conclusion and recommendation on consumer protection
D. Privacy (personal data protection)
   Cross-border transfer of personal data
E. Data protection (commercial and official data)
F. Remote Notarization
G. Cybercrime and cybersecurity
H. Electronic payments
   3. Foreign payments
I. Dispute resolution
J. Civil liability: private enforcement of good conduct

VI. RECOMMENDATIONS FOR DEVELOPMENT OF THE LAW

Responding to challenges: overview of policy dynamics

A. The statutory framework
B. Longer-term government plans
C. International issues

CONCLUSIONS

APPENDIX: ADOPTING THE E-COMMUNICATIONS CONVENTION AS DOMESTIC LAW

GLOSSARY

ADB	Asian Development Bank
APEC	Asia-Pacific Economic Cooperation (organization)
ASEAN	Association of Southeast Asian Nations
CAREC	Central Asian Regional Economic Cooperation (project)
CEFACT	Centre for Trade Facilitation (of UN/ECE)
CISG	(United Nations) Convention on the International Sale of Goods
ECC	Electronic Communications Convention (United Nations), more formally the United Nations Convention on the use of Electronic Communications in International Contracts
EIF	Enhanced Integrated Framework

ICT	Information and communications technologies
IETF	Internet Engineering Task Force
ISO	International Standards Organization
ITC	(United Nations) International Trade Centre
JSI	Joint (Statement) Initiative (of the WTO)
MDDC	Mongolia: Ministry of Digital Development and Communications
MFA	Mongolia: Ministry of Foreign Affairs
MLEC	UNCITRAL Model Law on Electronic Commerce
MLES	UNICTRAL Model Law on Electronic Signatures
MLETR	UNCITRAL Model Law on Electronic Transferable Records
OECD	Organization on Economic Cooperation and Development
RCEP	Regional Comprehensive Economic Partnership
TFA	Trade Facilitation Agreement (of the WTO)
UN/ECE	United Nations Economic and Social Commission for Europe
UN/ESCAP	United Nations Economic and Social Commission for Asia and the Pacific
UNCITRAL	United Nations Commission on International Trade Law
UNCTAD	United Nations Conference on Trade and Development
WTO	World Trade Organization

INTRODUCTION

The era of Covid-19 has underlined what the world already knew, that the way to more effective and efficient trade, both domestic and foreign, runs through electronic communications. However, innovative business methods using such communications often encounter legal frameworks designed for paper or print media. These encounters can lead to uncertainty and sometimes to barriers to efficient transactions.

Over the past quarter century, the legal frameworks have been adjusted to accommodate and even to promote electronic transactions. Considerable efforts have been made at the international level to develop and harmonize these initiatives, notably through United Nations organizations such as UNCITRAL – the UN Commission on International Trade Law - and UNCTAD – the UN Conference on Trade and Development. Regional initiatives have come from the UN Economic and Social Commission for Asia and the Pacific – UN/ESCAP – and the Association of South-East Asian Nations – ASEAN. International financing organizations like the Asian Development Bank (ADB) and the World Bank have also been involved, and more recently the World Trade Organization (WTO) and the Enhanced Integrated Framework (EIF).

Regulators and traders all recognize that technology evolves more quickly than business practices, and laws that support the business practices also need to evolve to continue their usefulness. Commercial law in general tends to validate changing practices rather than controlling what practices are allowed to develop.

Where the pace of change makes specifying rules in detail difficult, there is a premium on knowledgeable flexibility. Legislation around the world governing e-commerce has become less prescriptive and more permissive over time. The challenge is to prescribe what needs to be prescribed - clear authority to do new things, precise protection of interests that need protection – and to permit individuals and businesses to transact as freely as they can within that framework.

The Asian Development Bank (ADB) has engaged us to review and report on the legal framework for e-commerce in Mongolia, with a view to helping ensure that its content – statutes, decrees, orders, decisions - serves the country's purposes. In particular, our mandate is to identify legal and regulatory barriers to effective and efficient e-commerce and to develop recommendations for improvement.

All in all, Mongolia has made good efforts to keep up with changing times. It has opted for clarity when given the opportunity. Its most recent initiatives continue in that vein.

The present report reviews the legal framework of Mongolia related to electronic commerce from several aspects: electronic transactions, electronic signatures, trust services – and considers how traders and regulators have managed to operate under the law. It also considers the international legal context that importers and exporters must reckon with and the opportunities it may give for expanded operations.

The report also reviews the potential framework for a legislative regime on electronic commerce, starting with the need for a law on the topic at all, and examining a number of particular elements of e-commerce that deserve special attention, including consumer protection, privacy and cybercrime. It concludes with recommendations for the direction of law reform in the future.

It is often noted that Mongolia does not have a commercial law, other than the Civil Code. It does not have legislation addressing business-to-business transactions. The Ministry of Justice and Home Affairs and the Ministry of Economic Development have a project to develop a commercial law, i.e. B2B law.[1] The project was described in October 2022 as being in its late stages.[2]

Likewise, Mongolia does not have a trade law, one to deal with cross-border commerce. Efforts have been made to develop one over the years, and the Asian Development Bank recommended the adoption of such a law, and proposed a draft, in 2016.[3] To date, nothing has been adopted.

In the absence of a business-oriented commercial law or an internationally oriented trade law, this report considers the merits of a law focused on the operation and regulation of electronic commerce.

[1] The project is mentioned in a publication of the Mongolian Bar Association in February 2020: "Dr. Hartmut Fischer, The Systemisation of Commercial Law is of Economic Significance", online: https://www.mglbar.mn/news/3640?fbclid=IwAR0YHizkRTo4TKJmr4bb7hz2tqN1HvncBeu-jRsjuNB_uCE5VufX9EwUD3k.

[2] The project was mentioned in a meeting with a Japanese delegation on *Oct 27 2022: "* Secretary of State P. Sainzori received representatives of the Ministry of Justice of Japan," online: https://mojha.gov.mn/?p=8834&fbclid=IwAR2VwynirOH0KmyoZk2j2iMm7B21haLFy6cb95YaOa1POWUf1Vrs8j6nlxU.

[3] ADB, "International Trade Strategy for Mongolia", Rotterdam, July 2016. SOURCE: ONLINE? Annex 1: draft law on trade.

It will be noted that this report does not include an evaluation of the technology now deployed or potentially required in order to carry out effective and efficient e-commerce in Mongolia. The best laws will not produce good results if participants in the market cannot take advantage of them for lack of equipment, access to communications networks or skills to use them.[4] Likewise, lack of trust in intangible media, whether cultural or practical, can undermine business and consumer willingness to go adopt the most efficient business methods.[5]

Mongolia also faces serious challenges in delivering goods in its sparsely-populated regions where online merchants may have difficulty identifying where goods should be delivered and getting them there. This is not a problem that allows for a legislative solution, at least until technical infrastructure in the forms of usable addresses is built. The Law on the Post and the Law on Addressing frame parts of the problem. A committee of government experts is working on an addressing system as this report is being prepared, but no conclusions have been reached at time of writing.[6]

[4] The CAREC Institute has recently (March 2022) published a study of e-commerce infrastructure in the member states of the CAREC Program, including Mongolia. Many statistics on the state of technology and popular trust are reported, along with recommendations for improvement. *E-Commerce in CAREC Countries: Infrastructure Development*, CAREC Institute and ADB, March 2022, online: https://www.adb.org/sites/default/files/publication/781526/e-commerce-carec-countries-infrastructure-development.pdf.
It may also be that the project will be able to rely on technical analysis conducted for UNCTAD in its e-Trade readiness project study on Mongolia (forthcoming, 2023.) The collection of such studies is online: https://unctad.org/topic/ecommerce-and-digital-economy/etrade-readiness-assessments-of-LDCs.

[5] ADB and United Nations (UN) Economic and Social Commission for Asia and the Pacific (ESCAP). Manila, 2018. Embracing the E-Commerce Revolution in Asia and the Pacific. https://www.adb.org/sites/default/files/publication/430401/embracing-e-commerce-revolution.pdf .

[6] Construction: ministry of construction, city planning, internet development meeting report, Online: https://www.facebook.com/Barilgiinyam/posts/pfbid02rTt7ctw8CAe97ZhRpG22Sqvo2Mqixpxszg7wWUTUbdv7JGpHYHt3QEEGQQSNEkqql.

I. WHAT IS ELECTRONIC COMMERCE?

A. International definitions

Designing a legal framework for electronic commerce needs to start with a common understanding of what e-commerce is. There is broad but not complete consensus on that question among international organizations.

The World Trade Organization uses a definition first devised in 1998:

> Electronic commerce, or e-commerce, is defined as the "production, distribution, marketing, sale or delivery of goods and services by electronic means" (1998). An e-commerce transaction can be between enterprises, households, individuals, governments and other public or private organizations.[7]

The Organization on Economic Cooperation and Development (OECD), a private sector body, has a slightly narrower definition, used consistently since 2011:

> An e-commerce transaction is the sale or purchase of goods or services, conducted over computer networks by methods specifically designed for the purpose of receiving or placing of orders. The goods or services are ordered by those methods, but the payment and the ultimate delivery of the goods or services do not have to be conducted online. An e-commerce transaction can be between enterprises, households, individuals, governments, and other public or private organisations

E-commerce is a type of digitalization that amount to "...the sale or purchase/ procurement of goods or services, (includes getting estimates, negotiating, ordering, arranging contracts); electronic data interchange (EDI); mobile commerce; integration of ordering system with that of customers/suppliers; integrated invoicing and payment by customers; full integration with back-end systems; use of an extranet; secure transactions; automated payment of suppliers[8], conducted over computer networks by methods specifically designed for the purpose of receiving or placing of orders". Payment and delivery do not have to be conducted online. Orders made by telephone calls, fax or manually typed e-mail are excluded. An e-commerce transaction can be between enterprises, households, individuals, Governments, and other public or private organizations. (OECD (2011))

[7] World Trade Organization, online: https://www.wto.org/english/thewto_e/minist_e/mc11_e/briefing_notes_e/bfecom_e.htm

[8] https://unctad.org/system/files/official-document/dtlstict2021d2_en.pdf

The OECD excludes sales or purchases done physically or not using digital network means (webpages, extranets, electronic data interchange [EDI] networks). For example, orders by telephone calls and manually typed emails are excluded.[9]

The United Nations Economic and Social Commission for Asia and the Pacific (UN/ESCAP) discusses cross-border paperless trade in similar terms:

> [the] conduct of trade activities on the basis of electronic rather than paper documents e.g., electronic Customs declaration, electronic certificates of origin (all being applications of e-commerce to the international trade domain, such as in digital customs systems, an electronic Single Window facility, or e-port management systems.)[10]

The terms 'electronic commerce" and "digital trade" are often used interchangeably. Thus the Australian government defines both terms to mean "the trade of goods and services using the internet including the transmission of information and data across borders."[11] Note that it does not have to be international.

The United States International Trade Commission defines digital trade as "the delivery of products and services over the Internet by firms in any industry sector, and of associated products such as smartphones and Internet-connected sensors."

The common element of these national and international definitions is that e-commerce is simply ordinary commerce, buying and selling goods and services, using electronic communications rather than paper documents or speech. No special content of the communications is involved or required, nor any special technology.

Some sources would suggest a broader scope for the concept, beyond buying and selling.

> E-commerce is described as buying and selling products and services using the internet or online social networks. It creates relationships for value between businesses and individuals through electronic communications (Rahman, 2014). E-commerce includes

[9] *E-Commerce in the World Trade Organization*, online: https://www.iisd.org/system/files/publications/e-commerce-world-trade-organization-.pdf.
[10] ESCAP, online: https://www.unescap.org/sites/default/d8files/2021-01/CPTA.pdf

[11] Australian Department of Foreign Affairs and Trade, quoted in *E-Commerce in the World Trade Organization*, footnote 4.

> mobile sales, e-transactions, supply chain management and online transaction process (Sridhar, 2017).[12]
>
> E-commerce is not only buying and selling products and services over the internet but also involves other activities to support the sales process (Banda,2019)[13]

Another source says that trade focuses on the transaction; commerce may also focus on the broader economic activity.

> commerce includes all the activities necessary to facilitate trade, which means to deliver goods or services from manufacturers to consumers. Such activities include arranging transportation, providing banking and insurance services, promoting the products via advertising and storing the product in warehouses, etc. to complete this entire process successfully.[14]

As a result, the expression "e-commerce" tends to refer to all of those activities when conducted through electronic means of communication, whether or not they might be part of "trade."

However, these activities, when electronic, do not need additional legislative or regulatory support, beyond what frames their operations using traditional media. The "activities to support the sales process" are authorized in electronic form by a law that covers e-transactions and e-signatures, which – as discussed below – Mongolia already has.

"Trade law" is more likely to be used for the law of cross-border transactions and often includes in that context trade facilitation, trade protection, tariffs and customs matters. The international dimension of e-commerce, or e-trade, is discussed in Section 3, below.

What is the impact of the communications becoming electronic?

B. The nature of electronic communications

[12] AUTHOR TBD "E-commerce in Mongolia" CHECK TITLE, (2021), 17 Jl of Intl T&C No. 1 p. 68 (Feb 2021)
[13] Footnote 9, p. 69
[14] Vedantu, "Difference between trade and commerce", undated, online: https://www.vedantu.com/commerce/difference-between-trade-and-commerce. See also Key Differences, Surbi S, "Difference between trade and commerce", 26 July 2018, online: https://keydifferences.com/difference-between-trade-and-commerce.html.

Electronic communications differ from communications on paper in important ways that have challenged the application of traditional rules of law to them.[15] Understanding these differences will help explain why states, including Mongolia, have responded with the legislation they have and what measures are appropriate for further development.

Invisible processes. Electronic communications are created through the use and interpretation of electronic signals. This provides numerous benefits to commerce and the public at large. The main challenge in law arises from the fact that the computations used to deliver text and numeric information are invisible. Users have to trust the computers involved to do it right, and to do it the same way every time—i.e., to display on the screen or to send to the printer the same text for every party to a transaction and everyone else with an interest in it, such as auditors, regulators, and tax authorities. However, bits and bytes can degrade or be changed undetectably, leaving the resulting screen or paper text looking as perfect as the original. This is not the case with paper, where it is difficult to amend an original document without leaving a trace.

Rapid evolution of the technology. What one understands about the operations and risks of technology today may not be true tomorrow.

Legal uncertainties and doubts. Any user of a computer connected to a communications system may have cause to worry about intrusions into the computer for malicious or even criminal purposes. Consumers also wonder whether what they might buy online will be what is delivered to them, as well as whether they will have any remedy against a remote online merchant if the product that arrives is bad. The question for the merchants may be whether their remote online customers will pay them. Many of these issues arise with distance selling offline, such as by mail or telephone orders. Similar consumer protection measures may be useful.

Concern about misuse of personal data. It is easy for operators of electronic communications systems to "harvest" the data about individuals engaged in such communications. Not everyone trusts the legal rules set up to keep the collection, use and disclosure of personal information within acceptable bounds.

Different approaches and rules in different places. Electronic information crosses borders easily, but the rules for resolving its legal status may differ from one place to the next, and

[15] World Economic Forum, *Making Deals in Cyberspace: What's the Problem?*, White Paper, October 2017. Online: https://www.weforum.org/whitepapers/making-deals-in-cyberspace-what-s-the-problem

arranging for recognition of the effect of foreign rules has been difficult. Moreover, methods of resolving disputes may differ, though there are means of harmonizing them that are discussed later in this report.[16]

The result of these and other uncertainties have been unwillingness by some individuals and some businesses to trust electronic communications and e-commerce and a belief that the laws that apply to paper communications are inadequate to ensure confidence in the integrity of the products of electronic communications. When electronic communications first appeared in commerce, the existing laws protecting the integrity of paper documents did not fit them well or were difficult to apply.

Since the 1990s, however, a good deal of international consensus has developed on how to manage the transition of legal frameworks to electronic communications. In addition, e-commerce transactions have expanded all over the world even in the absence of supporting legislation. The question here is how to remove the remaining barriers—those governing electronic transactions—and channel e-commerce in a way that encourages its growth in a safe, sustainable manner.

This report discusses the international best practices – legislative and other – and indicates what may still be missing to optimize Mongolia's ability to manage commercial e-communications in its legal system.

Moreover, private technology will continue to offer new methods of doing e-commerce more securely. The law should leave room for the use of devices, codes, and platforms that are yet to be developed but that could avoid the need for some state regulation or administrative supervision.

Continuing dialogue between the private and public sector, including development partners, is important. For example, the United Nations Conference for Trade and Development (UNCTAD) has its ongoing "e-trade for all" program, which includes a private sector advisory group, to optimize and support public policies for e-commerce development worldwide.[17]

[16] See section V.I, text at footnote 271.
[17] Etrade for all, Online: https://etradeforall.org/. A recent description is found in D. Crosby, "Private Sector Views on Priorities for E-commerce," online: https://unctad.org/system/files/non-official-document/dtl_eWeek2017p15_DanielCrosby_en.pdf

UNCTAD is currently completing an Assessment of Mongolia's readiness for e-commerce. Its results will provide illumination of the points made in this report.

UN/ESCAP's technical and legal advisory groups can play a similar role.

C. What is an e-commerce business?

According to the definitions above, anyone capable of transacting with legal effect might engage in electronic commerce. Some of the definitions would require more advanced technology than others. However, an interactive website would suffice. It is often the case that enterprises will do business electronically through online trading platforms that provide technical infrastructure and often the promotional and transactional support as well. Such platforms are discussed later in this report. The platforms themselves are sometimes described as "e-commerce service providers" – a subset of e-commerce business with a key role to play in how e-commerce is conducted.

Governments often wish to encourage businesses to go online, to promote efficiency and lower transaction costs. In doing so, governments may have in mind that online transactions can produce more reliable records than paper-based deals, and websites and platforms may provide a means by which audits can be done and accountability of businesses to their customers and to public policy (e.g. payment of taxes) can be enforced.

This report will discuss how one might decide who qualifies for such encouragement and how to put such decisions into practice.

D. LAW OF ELECTRONIC TRANSACTIONS

A. Electronic Transactions

International best practices

Best practices in this area derive principally from the UNCITRAL Model Law on Electronic Commerce,[18] as confirmed by the UN Electronic Communications Convention.[19] The Model Law says that information shall not be denied legal effect, validity or enforcement solely on the grounds that it is in the form of a data message (i.e., in electronic form).

In 1996, UNCITRAL adopted the Model Law on Electronic Commerce (MLEC), which has been implemented in more than 80 countries and remains the best template for e-commerce legal reforms.[20] Because it is a model law rather than a convention, the MLEC can be applied by any legal system and adapted to fit into any legislative regime. The MLEC deals principally with form requirements, rather than with rules of substantive law. The MLEC also leaves a good deal of autonomy to transacting parties to decide how to satisfy its rules.

Electronic documents: The main challenge to the validity and use of e-documents has often been legal requirements that certain documents be in writing. UNCITRAL's MLEC provides that electronic documents can satisfy that requirement when their information is accessible and usable for subsequent reference. Another barrier to the use of e-documents is the common requirement for the original versions of documents to be produced for legal purposes. The MLEC provides a method of analyzing information in electronic form to decide if it is a functional equivalent of a paper original, i.e., can the electronic version achieve the policy goal (the function) that lies behind the traditional legal rule? The key element for a functional equivalent to writing, according to UNCITRAL, is whether the information can be shown to have retained its integrity from the time it was created until the time of analysis.

[18] UNCITRAL, Model Law on Electronic Commerce, 1996, online: https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce
[19] UN Convention on the Use of Electronic Communications in International Contracts, 2005, online: https://uncitral.un.org/en/texts/ecommerce/conventions/electronic_communications
[20] Footnote 18.

Sales

As noted above, the basic activity of electronic commerce is the commercial transaction, often a contract of sale from one party to another. Most of the substantive law of sales is "media neutral" – it can apply to paper-based or online transactions equally. As a consequence, questions of capacity of parties to contract (e.g. age, sobriety) or the mental element in a contract (e.g. consent, knowledge of what is being contracted for) are not different for electronic commerce than for transactions documented on paper.

General sales law is governed by the *Civil Code of Mongolia*.[21] The *Civil Code* does not require transactions to be in writing – they may be oral. If a transaction is put in writing, the written document does not need to be signed in order to be legally valid,, though most parties sign their transactional documents as a matter of prudence: a signature makes it easier to demonstrate attribution (origin) and consent if there is a dispute later.

This section of the report considers the nature of electronic transactions and of electronic signatures, in the Mongolian context.

The writing requirements in parts of the Civil Code are no longer a barrier to e-communications. The Code was amended in 2011 to provide that that transactions that are required by law to be registered, notarized, or in writing may be made electronically.[22] A number of provisions of the Code deal with specific kinds of contract, and many of them require a notarial signature and notarial registration – to begin with, in the notary's own files, but eventually in the archives of the Chamber of Notaries. The Law on Notary was amended in 2019 to ensure that notaries could perform these tasks electronically.

> A notary shall engage in notary electronic activities by making electronic registration creation information, uploading and enriching it to the database ... transmitting it to the state registry …[23]

There may be some concern that this provision covers only the registration of notarial acts, without authorizing the affixing of a notary's electronic signature to authenticate or certify the document. However, a compelling argument can be made that the Civil Code's express permission to

[21] The *Civil Code of Mongolia* is online: https://legalinfo.mn/mn/edtl/16147365399641
[22] *Civil Code of Mongolia*, art. 42[1].1. The current language on this point dates from 21 May 2021.
[23] *Law on Notary*, Mongolia, s. 25.2, online https://legalinfo.mn/mn/detail/400

perform electronically transactions requiring notarization must mean that the notary can do everything necessary to support a valid transaction, including incorporating an electronic or digital signature into the certified document.

Moreover, in article 43.2.4, discussing written agreements, the Civil Code provides that for electronic transactions, parties shall sign an electronic signature in accordance with the Law on electronic signatures as enacted in 2021 and in force in 2022.[24] So while transactions on paper may not need to be signed, almost all electronic transactions are signed, whether or not a notary is involved. We will turn shortly to a review of the law of electronic signatures in Mongolia.

Trading platforms

While individuals and single businesses may use a single Internet connection to communicate electronically to buy or sell goods and services, they may often find it difficult or overly time-consuming to make all the necessary arrangements for themselves. As a result, entities known as trading platforms have grown up to serve as commercial intermediaries.[25] Trading platforms allow many merchants to offer their wares to customers in one "place" and allow customers to buy them.

While the main global trading platforms are available in Mongolia – such as amazon.com and alibaba.com, they are used mainly for buying things online. There is not yet a reliable method to receive payments from outside the country, so cross-border selling for export is rare.

There are a number of Mongolian platforms, though the global platforms are considerably more popular.[26] One prominent example is shoppy.mn.[27] They offer a wide range of goods and services to all markets. They usually also provide some consumer protection measures, such as policies on returning or exchanging unsatisfactory goods – limited in main to deliveries to Ulaanbaatar.

> [Other platforms] include Ard shop, Unegui.mn, Mart.mn, and UBShop.mn … Also, most chain stores had their own online (e-shop). In addition, with the outbreak of the COVID-19, the social network began to play a huge role in e-commerce. As most of the population

[24] *Law on electronic signatures*, 2021, online: https://esign.gov.mn/law-of-signature. See discussion of e-signatures in the next section.
[25] Trading platforms should be distinguished from communications intermediaries through which Internet uses get online, notably Internet Service Providers, telecommunication companies, and others.
[26] Draft UNCTAD e-trade readiness study on Mongolia, forthcoming, 2023.
[27] Shoppy is online and described in its About and Frequently Asked Questions pages: https://shoppy.mn/about and https://shoppy.mn/support.

use social networks, it has become very convenient for companies to reach their consumers through these networks. The study that … conducted survey among 500 participants of Ulaanbaatar points out that 43% of consumers use Facebook to buy goods and services for their personal consumption, and 6% use Instagram.[28]

At present Shoppy.mn and the other platforms are all their own "electronic ecosystems" with proprietary logistics, warehouses and even consumer credit providers. They not governed by dedicated law but only by general commercial standards set out in the civil and criminal law. Whether more is needed is discussed below in Part V, Regulatory Framework for E-Commerce.

B. Electronic Signatures

International best practices

The international legal framework for electronic signatures starts with the UNCITRAL Model Law on Electronic Signatures (MLES),[29] as updated by the U.N. Electronic Communications Convention (ECC)[30] in 2005. These documents provide that where the law requires a signature, an electronic signature will satisfy the requirement if the electronic method of signing reliably identifies the signatory and indicates its intention with respect to the signed document.

Both the MLEC and the ECC provide rules on what may make an e-signature reliable. The signing device must be associated only with the signatory; the device must be in the sole control of the signatory, and any change to the signature (and sometimes the document) after signing must be detectable. (MLES 9.6))[31]

At the higher end of the reliability scale are digital signatures, described below.

[28] From PUREVSUREN, Khash-erdene. "E-Commerce Policy in Mongolia : Analyzing the E-Commerce Law of the Republic of Korea for Successful Experience to Consumer Protection in Ecommerce of Mongolia" - by M.A. thesis in public policy, Korea.

[29] UNCITRAL Model Law on Electronic Signatures, 2001, (MLES), online: https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures (in Mongolian).

[30] Electronic Communications Convention, footnote19.

[31] The MLES says that where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, then any alteration to that information needs to be detectable too. Article 6(3)(d). Not all legal systems expect a signature to support the integrity of the signed information.

While contracting parties in Mongolia do not need to sign their written transactional documents, it remains prudent for them to do so. The Civil Code says, however, that users of electronic transactional documents must use an electronic signature within the meaning of the *Law about Electronic Signatures.* Once one signs an electronic document, the signature is governed by that *Law*.[32]

It should be noted that the terminology on the types of signatures is inconsistent among the statutory and explanatory documents. The Mongolian words for "electronic signature" are цахим гарын ("tsakhim garyn"). The words for "digital signature" are тоон гарын ("toon garyn"). Translation programs like Google Translate and Word are inconsistent and sometimes even contradictory in how they interpret both phrases. The Civil Code uses the term "electronic (цахим) signature". The statute on signatures is called the Law on Electronic (цахим) Signatures, though it is frequently referred to, even in English publications in Mongolia, as the Law on Digital Signatures. It is not clear that the issues of usage are only a matter of translation; the texts themselves sometimes appear uncertain.

The Law on Electronic Signatures defines an electronic signature as "electronic data attached to or combined with the information in order to identify the person who signed the electronic information."[33] Apparently any electronic method of associating an identified legal entity meaningfully with a text is such a signature.

However, a digital signature is defined as an "electronic signature that meets the requirements set out in Article 6.2 of this Law".[34] Article 6.2 sets out three requirements:

6.2.1 The information [must be] created through encryption and conversion using a private digital signature key (hereinafter referred to as "private key")

6.2.2 [One must] be able to identify and verify the digital signature certificate holder… using the digital signature public key (…"public key").

[32] Civil Code of Mongolia, footnote 21, article 43.2.4. See the *Law about Electronic signatures* (2021), footnote 21.
[33] Footnote 24, art. 4.1.10.
[34] Footnote 24, art. 4.1.3.

6.2.3 [One must] be able to know whether the digital signature has been attached to the information to be signed, and whether the information has been modified after the signing process,[35] and whether the information is complete.[36]

The use of a digital signature has the same legal effect as using a handwritten signature.[37]

While the official government website on e-signatures acknowledges the existence of electronic signatures that are not digital signatures,[38] electronic signatures are not given any explicit statutory effect, at least not in the Law on Electronic Signatures. It could be argued that this function is served by the Civil Code provision giving legal effect to an electronic document so long as it is signed with an electronic signature within the meaning of this statute.[39] Neither statute gives an express indication of why a transacting party would choose one type of signature rather than another – except of course the statutory validation of the digital signature in article 6.3, just mentioned. Digital signatures are not prescribed for any purpose.

Individuals may have the means of creating digital signatures and may use such signatures. The properties of a digital signature are prescribed by law.[40] Organizations and businesses, known as "entities", use a digital seal instead.[41] Technologically they are consistent with digital signatures. Their operation is described in the statute in general terms.[42] There are rules for cases when the entity does not have a seal and a human being has to sign for the entity with a personal digital signature.

[35] This sub-article of the statute refers to "consolidation" or "merging", which reflects the way a digital signature is generated: the compressed message and the signing key are combined to make a unique digital object, the signature.
[36] The integrity of the signed message is supported by doing a mathematical compression or "digest" of the message, called a "hash". There are standard hash creation algorithms available, and a digital signature device should come equipped with one. If anything in the message is changed, then it will not hash to the same result. So the recipient verifies the digital signature by rehashing the message to see if is the same. If not, the rehashed message will normally not be comprehensible. See "What Is a Hash Function in Cryptography? A Beginner's Guide," online: https://www.thesslstore.com/blog/what-is-a-hash-function-in-cryptography-a-beginners-guide/
[37] Footnote 24 article 6.3.
[38] Ministry of Digital Development and Communications (MDDC), E-Sign home page: online: https://esign.gov.mn/?s=PKI&submit=
[39] One should consider article 196.1.8 of the Code as well.
[40] Footnote 24 article 8.
[41] Footnote 24 article 6.5. Other rules for and characteristics of digital seals appear in article 7. Some translations refer to a "digital stamp". (Neither "seal" nor "stamp" is literally correct, since those words refer to something done to paper. The usual term in the literature is "digital seal." Its function is to make the information safe from alteration.)
[42] Footnote 24 article 7.

More information on the technical operation of digital signatures is found in the next sub-section of this report, below.

Digital signatures are accompanied by certificates that attest to the identity of the holder of the signing data (the "certificate holder"). The full contents of the certificate are set out in the statute.[43] The rights and obligations of the certificate holder are also matters of statute.[44] See the discussion of Trust Services, below.

What all this may mean in practice is that people may not be able do business electronically – even a simple person-to-person transaction – without acquiring the means to make a digital signature, including a certificate. The Law says, however, that "no limit shall be established on the type of digital signature device." MDDC is to prepare and make public "the type of digital signature device that meets the requirements."[45] It is not clear that any such statement has been issued as of late 2022. Nor is it clear what potential devices might be available in any event. However, such a statement by MDDC might enable business-to-business transactions to use simple or accessible forms of digital signatures. It might also allow signed transactions on electronic trading platforms.[46]

Any freedom of choice implies some capacity on the part of signatories to transactions to appreciate computer security, to choose the appropriate level of reliability and to be able to keep the signature data safe. A certificate may be suspended or revoked if its holder does not keep it secure.[47] In addition, one needs to be able to verify the status of a digital signature on an electronic document that one receives.[48]

Mongolian law on electronic signatures can be technology neutral, as many international best practices stipulate[49], in that it allows for the use of any kind of e-signature. However, the statute generally focuses on and prefers digital signatures, which are not technology neutral. They rely

[43] Footnote 24 article 10.
[44] Footnote 24 article 14.
[45] Footnote 24 article 8.5. An alternative translation suggests that MDDC is to list the devices that are acceptable. Such specificity seems unlikely. Some translations speak of "tools" rather than "devices" for creating electronic signatures. Where technology is involved, "devices" is the preferable term. The word in Mongolian is the same in all cases.
[46] It appears that buying and selling does go on via trading platforms, even in the absence of any digital signature. Either the transacting parties rely on the more general permission of the Civil Code, or they are satisfying themselves of reliable authentication by less formal means.
[47] Footnote 24 article 18.1.6, for breach of provisions of article 14.3.
[48] A list of expired and invalid digital certificates is on the Ministry's e-sign website: https://esign.gov.mn/#intro. [The Chrome browser will translate the page on request.]
[49] See for example discussion in section IV.A.1, text at footnote 139.)

on a particular kind of cryptography which carries with it an array of technical standards and expectations.

Whether this creates problems in transacting is discussed in Section II, below, on E-Commerce in Practice.

One may conclude that the Mongolian Law on electronic signatures conforms only in part to international standards. It offers a good deal of flexibility to transacting parties, but without much guidance on why one might want to use one kind of signature technology rather than another. It does not clearly leave the choice of technology to parties, whatever the value or importance of the document to be signed. However, the Law does help citizens who want to communicate with the government or public agencies. That topic is discussed in more detail below.

The use of digital signatures among related parties is not so strictly regulated, however. Article 5.3 of the Law on Electronic Signatures says this: “If a legal entity uses a public key infrastructure for its internal operations, it is not necessary to obtain a special license” (meaning a certificate from an authorized certification body.) So for internal purposes, a company or organization could acquire off-the-shelf digital signature software.

One challenge in making digital signatures the only form of e-signature with statutory validity (even if there may be a variety of digital signing devices with this benefit) is to ensure that a good number of people are able to create digital signatures. How easy is it to acquire a signing key and a certificate?

The government has had a program of distributing digital signing data to citizens, embedding the data and certificate in the electronic version of the national identity card. The contents of certificates for citizens and others are set out in article 10. For citizens able to get such certificates, digital signatures would not be a problem. However, many people outside Ulaanbaatar were not able to get the signature data, and the free distribution of such signing data has apparently ended.

While digital signatures can be very secure and thus trustworthy, if they are difficult, or even expensive, to use, then it may be preferable that not all transactions should require that degree of security. One could decide to leave the decision about the quality of the e-signature to transacting parties. This is so particularly where there is no great public interest in the transactions that the signatures support.

The importance of the transaction, or of any other occasion on which a signature is required, may be judged by a number of factors: the nature of the parties - is one a public agency? The value of the transaction: how much is at risk if the signature is false and the transaction fails? The risk of failure as judged by the parties: do they know each other, have they done business before, is the amount of money in the transaction high or law?

The law can leave the evaluation of these factors to the parties, or it can prescribe some or all of them. The most common prescription in Asia is that interactions with government or parts of government need to have a digital signature. The certainty of identification and the integrity of the content of the signed document are both considered of high importance.

Statutes sometimes leave transacting parties a lot of discretion on their signing technology for routine transactions, whlle requiring more reliability – and thus more technology – for higher value deals and communicating with government or public agencies. Such statutes are often known as "hybrid" laws – partly general e-signature, partly digital signature.

For example, the Electronic Transactions Act of Singapore provides for digital and electronic signatures in different circumstances.[50] Japan[51] and India[52] do likewise. The European Union distinguishes between "qualified" and "unqualified' signatures based on similar criteria.[53]

In practice, Mongolians are making use of the digital signatures issued by the government in their communications with state agencies, and not in private transactions.[54] For other interactions, it may be appropriate to leave the judgment of the type of signature to the transacting parties.

It should be noted that Mongolian law contemplates a number of methods of 'authentication' beyond signatures covered by the Law on Electronic Signatures. It is possible that some of these methods could be allowed – by amended statute – to be used in commercial dealings as well, where digital signatures remain harder to acquire or use.

---

[50] Singapore, *Electronic Transactions Act, 2010 (revised 2020)*, online: https://sso.agc.gov.sg/Act/ETA2010 See section 8 on signatures and section 18 on secure electronic signatures.
[51] Adobe, *Electronic Signature Laws & Regulations – Japan*, online: https://helpx.adobe.com/legal/esignatures/regulations/japan.html
[52] Adobe, *Electronic Signature Laws & Regulations – India*, online: https://helpx.adobe.com/legal/esignatures/regulations/india.html
[53] European Union, *e-Signature FAQ*, online: https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eSignature+FAQ
[54] Conversation with Director Gantogoo of MDDC, 17 October 2022.

Most of these alternative methods currently apply in the public sector and depend implicitly on the reliability of public records. For example, the Law on the Transparency of Public Information[55] provides in article 19 that "When providing services to people and legal entities in electronic form, the State shall recognize the person and legal entity using electronic signatures and identification and login systems with methods and tools determined by the Government." This seems to permit the government to accept authentication methods other than digital signatures or indeed to accept anything that would resemble a traditional signature in electronic form.

Article 21.2 of that Law appears to allow persons from outside the government to log into and 'use the shared system for the exchange of official letters when sending and receiving official letters electronically in a form other than official e-mail."

The Law goes on to say in article 24.4 that "[a]n electronic document with a unique number issued by the unified system of state services is as valid as a paper document". No mention is made of a signature. The unique identifier issued by the custodian of the record is enough to justify the record's use by others.

Moreover, article 30 of that Law says "[u]nless otherwise provided by law, electronic documents are valid in the same way as paper documents." "State organizations and officials shall use the official e-mail and the support system provided for in Articles 21, 23, and 24 of this law when communicating electronically within the scope of their duties specified in the law."

Likewise, the Law on Archives[56] provides that electronic documents are to be certified by electronic signature or a unique number – the same principle as under the Law on Access to Public Information.

The Law on Money Deposits, Money Transfers, and Loan Activities of Banks and Sovereign Legal Trusts[57] says that passwords, secret codes and electronic signatures that meet confidentiality requirements may be used to provide services in electronic form, and that these are equivalent to handwritten signatures in electronic transfers and similar situations. It should be noted that the

[55] Law on Transparency of Public information, online: https://legalinfo.mn/mn/detail?lawId=16390263044601.
[56] Law on Archives and Official Management, article 38, online: https://legalinfo.mn/mn/detail/15370.
[57] Law on Money Deposits, Money Transfer and Loan Activities of Banks and Sovereign Legal Trusts, article 7.1, online: https://legalinfo.mn/mn/detail?lawId=16230554816671

financial institutions subject to this Law may provide online services only to customers with whom they have an enabling agreement signed on paper.[58]

In short, a number of government agencies are allowed to rely on the products of a number of methods of authentication that are not as complex or controlled as digital signatures under the Law on Electronic Signatures.

It may be that such flexible (and often technology-neutral) arrangements might be authorized for private-sector authentication as well, with suitable analysis of security considerations in different contexts. One thinks of transactions performed through electronic trading platforms: they do not use digital signatures. In fact, the digital signature system contemplated by the Law on Electronic Signatures is not yet in operation.

If trading platforms have any form of signature, it seems outside the scope of the laws discussed here so far. Article 196.1.8 of the Civil Code appears to provide broader flexibility than the Law on Electronic Signatures:

> 196.1.8. If the contract is concluded in electronic form, the parties shall make an electronic document expressing their will and sign it digitally, or by signing an electronic signature that mutually acknowledges the expression of their will using technical tools and software.

The second option in this article gives scope for innovation in what the parties may choose to accept: a kind of electronic signature that is not a digital signature.

The Ministry might also use article 8.5 of the Law on Electronic Signatures to designate types of digital signatures that would be effective for platforms.

It is also possible, for trading platforms, that the ability to order goods and to pay for them online is sufficient authentication for practical purposes. Merchants do not need to know who they are dealing with, so long as they are paid for what they sell. The forthcoming Law on consumer protection may also spell out some clearer rules about who has to identify him/her/itself to other transacting parties, with what consequences.[59]

It may be worth noting at this stage that the large number of transactional documents that the Civil Code requires to have notaries to validate them may suggest a distrust of (paper) signatures

[58] Footnote 57 article 7.
[59] See section V.C, text at note 210.

on their own. This attitude may support a low-risk approach to electronic signatures, i.e. a preference for digital signatures not just out of concern about the technology but in general about the whole signing/authentication process.

1. Digital signatures

As noted, perhaps the majority of electronic signatures created in Mongolia are, in technical language, 'digital signatures."' A digital signature is, as article 6(2) of the *Law about electronic signatures* puts it, "information created through encryption and conversion using a private electronic signature key ("private key").[60]

The cryptography involved is known as 'dual key' or 'public key' cryptography. The two mathematical keys are generated together (usually by a certification body) and function so that what is encrypted with one key (the "private key") can be decrypted only by the other (the "public key"). If a party known (usually because certified) to have one of the key pair signs something with that key, then someone decrypting the signature with the other key can be confident that it was signed by the party named in the certificate.

This system depends on the security of the signing device (e.g. computer, phone, tablet) containing the private (signing) key, so that nobody other than the certified party can sign anything with it. For that reason, the laws on the topic, including sub-article 14.3 here, require the certificate holder to "ensure the confidentiality and security of private keys" and that any compromise of the security of the signing device or of the signing data in the device must be reported to the certification body. That will almost certainly invalidate future signatures using that data (and to an extent past signatures as well, if they have not been relied on before the compromise is discovered.)[61]

There are other technical requirements for the usual use of digital signatures that are beyond the scope of this report.[62] Those requirements are very much in the mainstream of how digital

[60] Footnote 24 articles 4.1.3 and 6.2.
[61] Footnote 24 articles 14.3.2 and .3.
[62] A set of draft regulations on certificate management was issued in September 2022: National Public Key Infrastructure Draft General Rules; Draft Procedures for Creation, Use and Storage of Database of Digital Signature Certificates; Draft Registration Procedures; and Certificate Service Tariff Determination Methodology.

signatures are governed around the world.[63] While the UNCITRAL Model Law on Electronic Signatures that is the equivalent to the Mongolian legislation is phrased in technology-neutral language, i.e., it does not expressly require any particular technology to operate, in practice its provision on signatures presumed to be reliable is usually taken to describe digital signatures using public-key cryptography.

2. Trust services

Trust services support the authentication of electronic messages. Trust service providers are often issuers of the data (codes, encryption keys) used to create electronic signatures, and even more often the issuers of certificates that link the signature data embedded in an electronic signature with the person (natural or legal) or entity who used the data to sign something. A person's e-signature may be incomprehensible code, and the certificate interprets the code to say, "this signature belongs to X".

The trust services in Mongolia are called certification bodies, assisted by licence holders (licensed to issue digital signature certificates and supervise their operation).[64]

The "trust" in trust services is the trust generated in the person asked to rely on the e-signature that the e-signature is actually from the person it says it is from.

Some purposes of digital signatures may require more security than others, and thus more reliable technology and procedure.[65]

Moreover, some trust services will in practice be more trustworthy than others. That is why the electronic signatures law contains considerable detail about the establishment of certification bodies and licence holders, their duty of competence, security and procedural care, insurance coverage, the contents of certificates, and so on.

[63] Cybersecurity and Infrastructure Security Agency (USA), "How digital signatures work", updated 2020, online: https://www.cisa.gov/uscert/ncas/tips/ST04-018. A more thorough review of digital signatures in the context of global laws on signatures and authentication was published in 2007 by UNCITRAL, "Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods", online https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/08-55698_ebook.pdf. Digital signatures are discussed at pages 17 to 27.

[64] Footnote 24 articles 10 ("certificate"), 20 ("Certification body") and 23 ("Licence to provide a certification service").

[65] The literature of digital signatures often describes "levels of assurance' of different types of digital signature, though different trust services may have different names for their levels. Understanding the different levels of assurance of different public key infrastructures, and thus comparing their reliability, is complex and time-consuming.

The whole system of technology, rules and practices for issuing, securing and certifying digital signatures is known as a "public key infrastructure" or PKI.[66]

The statute sets out in detail the requirements of the office that issues digital signatures, called the certification body.[67] The requirements are intended to ensure technical expertise, financial stability (in case the body needs to satisfy judgments against it), and responsiveness to its tasks.

Moreover, the Ministry of Digital Development and Communications provides polices and regulations for the operation of the national public key infrastructure and the discipline of licence holders, i.e. certification bodies, as well as working to harmonize operations of the PKI with foreign countries and international organizations.[68] The Communications Regulatory Commission has higher-level duties to ensure the PKI has appropriate standards and procedures.[69]

The Mongolian rules on trust service providers are much like provisions on the same topic in other countries' statutes, and to a degree derive from similar provisions in the UNCITRAL Model Law on Electronic Signatures concerning the reliability of certification service providers.[70]

Most recently, UNCITRAL's Working Group on Electronic Commerce has developed a draft Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services,[71] adopted by the plenary session of UNCITRAL in June 2022. Its statements of the duties of identity managers (those who identify commercial participants and confirm their attributes) and trust service providers (articles 6 and 10 of the draft Model Law) may become the international best practices, given the success of UNCITRAL's formulation of such rules in the past. It may make sense for Mongolia to consider whether its laws should be consistent in principle with this new Model Law, especially where trading partners are influenced by European norms. It is too early to make a firm recommendation on the point.

Another international initiative that will become relevant to e-signatures in Mongolia and elsewhere is the agreed text on e-signatures and authentication that has been developed recently

[66] The technical operations of Mongolia's PKI are described at the Ministry of digital development and communications' website: https://esign.gov.mn/#intro i
[67] Footnote 24 articles 20, 21, 22.
[68] Footnote 24 article 31.
[69] Footnote 24 article 32.
[70] Footnote 24, article 10.
[71] The Model Law is online as document A/CN.9/1112, 21 February 2022: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/acn9-1112-e.pdf The Model Law will probably come before the General Assembly for final adoption later in 2022.

by the Joint Initiative on Electronic Commerce, a part of the World Trade Organization.[72] The text has not yet been turned into law ready for implementation, but it will influence legal developments over the next few years.[73]

3. Foreign signatures and certificates

The Mongolian statute reflects the Model Law on Electronic Signatures in its rules on recognition of foreign signatures. The Model Law says that foreign e-signatures should be as valid as domestic e-signatures, if they have comparable levels of reliability.[74] The Mongolian Law on Electronic Signatures speaks of foreign certificates rather than of signatures. Article 19 of that law treats a foreign certificate in the same way as a Mongolian one, on one of two conditions:

- There is official recognition by the Mongolian government that the foreign certification body meets the requirements set forth in the law and relevant regulations; or
- A certificate of a foreign certification body has been recognized by an international treaty to which Mongolia is a party.

While these criteria do not expressly focus on the similarity of level of reliability of the foreign e-signature, that seems likely to be the focus of any inquiry on either point.

At present, however, there are no such official recognitions and no such treaties, so in practice, foreign signatures or signatures with foreign certificates are not valid in Mongolia.

C: Other potential contents of e-Commerce legislation: international models

A law about electronic commerce should provide for the two major topics discussed so far: the legal status of "written" documents when they become electronic, and how to create a reliable electronic signature. As noted, Mongolia has legislated in both areas – though the e-signature statute would benefit from clarification about the occasions on which one should use an electronic rather than a digital signature, or vice versa.

[72] WTO, "E-Commerce negotiations: Members finalize 'clean text' on e-signatures and authentication", 20 April 2021, online: https://www.wto.org/english/news_e/news21_e/ecom_20apr21_e.htm.
[73] For further well-informed discussion on authentication and signatures, and much else, see the *Work Plan on the Implementation of ASEAN Agreement on Electronic Commerce* published by ASEAN in March 2022, online: https://asean.org/wp-content/uploads/2022/03/Work-Plan-E-commerce-Agreement_endorsed_logo.pdf.
[74] MLES Footnote 29 article 13.

However, the UNCITRAL Model Laws deal with other topics on which Mongolian law is silent. Mongolia may wish to consider whether some of these topics would serve the purposes of e-commerce practitioners in the country.

1. Information is not ineffective in law solely because it is in electronic form

This is UNCITRAL's "non-discrimination" clause,[75] a general rule that any information with legal effect can be in electronic form, if it meets other rules about its presentation and content. It helps resolve borderline questions in favour of allowing the electronic communications to be valid. It could support an argument that a provision on using electronic communication is in effect a functional equivalent to the traditional paper-based communication and thus valid for that reason.

2. Electronic evidence is admissible

Electronic documents may be valid, but parties may have to prove their validity, and their meaning, before a decision-makercourt. For that purpose, the documents must be able to be presented to the court or to another adjudicative body. UNCITRAL's rule in the MLEC[76] is that evidence is not inadmissible solely because of its electronic form. There are other criteria that one can apply to judge the strength of electronic evidence, beyond the scope of this report. At present, Mongolian law allows for e-evidence in some criminal matters and also in civil proceedings, without detail as to how to introduce it.[77] A.

3. Record retention rules apply to e-documents

Many rules of law require people or businesses to retain their records, perhaps for tax audits, regulatory inspections or in case of litigation. UNCITRAL's rule[78] is that electronic records will satisfy record retention rules if the records are accessible to the appropriate people for the same period as paper documents for the same purpose.

4. Time of sending and delivery of electronic messages

Electronic messages usually pass through communications intermediaries such as Internet Service Providers (ISPs) and other computers on their way from the sender to the recipient.

[75] MLEC Footnote 18 article 5.
[76] MLEC Footnote 18 article 9.
[77] Law on Civil Procedure, article 37.2, online: https://legalinfo.mn/mn/detail?lawId=302&type=11
[78] MLEC Footnote 18 article 10.

UNCITRAL provides rules[79] on who the "real" sender is, and when messages should be deemed to be received.

5. Electronic contracts may be made without human intervention

Offline, contracts are made by a seller and a buyer reaching an agreement. The Civil Code deems agreement to have been reached in certain circumstances. When people deal with a website, however, it may not be clear when a person accepts an offer, or perhaps the website is making the offer – but then can the site's offer be accepted by an unlimited number of people? UNCITRAL makes it clear that automated transactions are valid contracts, but that websites that can make such contracts are not making offers to the world that everybody can accept. They are invitations to the world to make offers, and someone sending a 'buy' message to the website is legally making an offer, not accepting one.[80]

6. Correcting mistakes when communicating with a machine

People sometimes make mistakes in communicating during negotiations. If a contract is made with a machine (e.g. the computer on a website), is there some way to make a correction, or is it too late? Is the contract made in final form and binding as soon as the message is sent to the seller's computer, even if by mistake? While the Model Laws did not address this question, the E-Communications Convention does.[81] It allows the right to withdraw the mistaken communication if the other party had not given an opportunity to review and correct the communication before it was sent, so long as the party making the mistake does not derive any benefit from the contract before correcting it.

Mongolia's Civil Code has a number of provisions about error, both negligent and as a result of misrepresentation. A rule like the ECC's article 14 could fit well into that list.

D. Other potential contents of e-Commerce legislation: Mongolian proposals

While UNCITRAL developed the two "minimalist" model laws reviewed above, it said clearly that other elements of electronic commerce might need to be regulated as well. Some were not dealt with by UNCITRAL because harmonization at the global level was not possible, and some because of lack of regulatory expertise. The fact that UNCITRAL did not provide model legislation

[79] MLEC Footnote 18 article 13.
[80] ECC footnote 19 article 11
[81] ECC footnote 19 article 14

does not mean that regulating such matters is inconsistent with the international standard. Such standards can and do come from other sources,

A workshop of private and public sector stakeholders in electronic commerce, those doing business online and those with regulatory responsibilities for it, was held in June 2022. The participants discussed the weaknesses of current Mongolian law and ideas for strengthening it. Most but not all of the participants from both the public and private sectors thought that a special law on e-commerce would be helpful, to create greater certainty and uniformity of practice.

Most of their ideas were practical or technical rather than legislative. The legislative list is set out here. More discussion of some of the ideas appears below in the section on the regulatory framework for e-commerce. The practical items are in the section immediately following this one.

The legislative implications are discussed further in later sections of this report:

- Fairness is needed between formal merchants and social media sellers, including tax fairness.
- Protection against fraud and cybercrime is generally needed. The Criminal Code has some provisions, and the new Law on Cybersecurity of 2021 (in force in May 2022) will be helpful. The topic is dealt with in the Framework section of this report.[82]
- Some product-specific issues of standards need resolution for online sales, e.g. for medical supplies.
- One government agency should be responsible for e-commerce.
- Laws should conform to international conventions.
- E-commerce law should fit into a general trade law, not yet in existence.

E. ELECTRONIC TRANSACTIONS IN PRACTICE

As noted, the laws of Mongolia have been becoming more accommodating to electronic commerce over the past decade or more. The text of legislation is not always reflected in commercial practice, however, for one reason or another. It may be that businesspeople are not aware of their opportunities to go electronic, or they lack the technical skills to do so, or they lack the computer equipment. The same may be true of their potential trading partners, at home or

[82] See section V.G, text at footnote 251.

abroad. Perhaps the permissions in the legislation are not clear enough to prompt a change of behaviour.

To estimate the gap, if any, between the legislative theory and the business practice, our team (notably Ms Delgermaa Anbat) helped the Ministry of Digital Development and Communications to organize a workshop of private sector and public sector stakeholders to talk about e-commerce in law and practice. This section notes her findings and our observations on them.

Practical observations of issues that need resolution to facilitate e-commerce included:

- Border issues – delays, closures impeding import and export of goods.
- Delivery generally is difficult and expensive, especially in remote areas.
- Quality assurance for goods and services is not reliable.
- Information security needs improvement.
- E-payments could be better: coordinate payment systems
- Fraud and fake websites are too common, but secure systems are expensive
- Signature data on a SIM card on a phone is easier to use than on an identity card. There are businesses in Mongolia that provide a SIM-based digital certificate. A consortium of Tridum e-Security[83] and Mobicom Corporation[84] have offered digital certificates embedded on their customers' SIM cards since 2019.
- Promotion and education of e-commerce would help people be more comfortable with it.
- Interoperability of systems is a practical and economic benefit to traders, regulators and customers.

A. The private sector

Many Mongolians shop online, from private sellers or private platforms. As noted earlier, they use both well known global platforms and a number run in and for Mongolia.[85]

Some of these platforms offer some protection to the interests of consumers who buy on the site. There is a limited right to return or exchange products, for example.[86]

[83] Tridum e-Security, online: https://www.tridum.mn/eng (click on Public Key Infrastructure)
[84] Mobicom Corporation, online: https://www.mobicom.mn/en?mid=453#/
[85] See the discussion of trading platforms, below, section V.B.2, text at footnote 189.
[86] For example, consider shoppy.mn, online at https://shoppy.mn/t/home and that site's FAQ question 9 (return) and 10 (exchange): https://shoppy.mn/support/faq

There is some evidence that the challenges to doing business electronically do not arise principally from deficiencies in the law but from practical, cultural and technological barriers.

On the cultural side, some buyers prefer to rely on ink signatures on paper, even though e-signatures are permitted by law. To some extent, businesspeople may be waiting to see if some of the regulations that may be made under the Law on Electronic Signatures and other new related statutes are workable for them. At present, the public key infrastructure contemplated by that law does not exist.

It will be noted that the Law on Electronic Signatures provides for digital signatures and signing data to be uploaded onto Mongolian citizens' identity cards, which then can be used to sign electronically.[87] A significant proportion of the urban population has taken advantage of this offer. However, most of the communications signed by these easily-obtained digital signatures are between citizens and public agencies. Very few if any are for private transactions.[88]

People doing transactions with the private sector, notably through trading platforms or directly with merchants, make their arrangements through the platform consents rather than written contracts. If there are contracts in writing, presumably they fall within article 43.2.4 of the Civil Code. Their signatures can be "in accordance with the Law on Electronic Signatures" without being a certified digital signature. No notary would be required for such a transaction.[89]

It will be noted that s. 196.1.8 of the Civil Code says a person is deemed to have entered into an agreement by expressing their interest by making an electronic document and signing it electronically, or by signing an electronic signature that mutually acknowledges the expression of their will using technical tools and software. The latter phrase may allow for contracts to be formed without the full digital signature arrangements.

Moreover, the Law on Electronic Signatures, as was noted earlier, allows MDDC to authorize different types of digital signatures as valid. Thus, the kinds of digital signatures used to transact on or with trading platforms could be expressly recognized for this purpose, if any doubt arose as to their validity.

[87] Footnote 24 article 8.4. Foreigners may have certificates – article 10.2.2 – but not to an identity card. Certificates stored on SIM cards, i.e. on mobile phones, should work for people of any nationality.
[88] Conversation with Gantogoo Zundui, Director-General of Policy and Planning, MDDC, 17 October 2022.
[89] If there were a case to be made for legislation on trading platforms, a provision validating the signatures used on and by the platforms might give reassurance to anyone who needed it on this point.

Some of the barriers to e-commerce in the private sector are not legal but technical, or perhaps economic.

On the technology side, there is broadband Internet access of variable quality in the country, especially for mobile connections. There is some satellite service for herders in remote areas. Even when connected, however, there is some distrust of the fate of one's personal information through online shopping. That may be helped by the new privacy legislation mentioned later in this report, if it is perceived to be workable.

The cost of delivery of packages bought online is high, even in the capital but seriously outside that city, which is another disincentive to buy through that medium.

B. The public sector

1. Single window

International best practices

The United Nations Centre for Trade Facilitation (CEFACT), part of the Economic Commission for Europe, has two main guides for countries developing a single window:

1. Recommendation 33: Establishing a single window [90]
2. Recommendation 35: Establishing a legal framework for a single window. [91]

The ESCAP Framework Agreement on Cross-Border Paperless Trade in Asia and the Pacific also encourages member states to establish a single window to facilitate and economize on the technical communications it deals with.

The WTO Trade Facilitation Agreement (TFA) likewise encourages member states to establish a single window for this purpose. [92]

[90] Online: https://unece.org/DAM/cefact/recommendations/rec33/rec33_trd352e.pdf
[91] Online: https://digitallibrary.un.org/record/668437?ln=en
[92] WTO Trade Facilitation Agreement article 10(4), online: https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/L/940.pdf&Open=True. Article 10(4.1): "Members shall endeavour to establish or maintain a single window, enabling traders to submit documentation and/or data requirements for importation, exportation, or transit of goods through a single entry point to the participating authorities or agencies."

One of the main activities that facilitates cross-border paperless trade is the creation of a "single window", which is a central clearing-house or communications hub for documents requiring regulatory approval, for imports or for exports. The importer, or carrier on behalf of the importer, or the exporter, can file (lodge) all documents for the destination country in one place, with one office, or – electronically – one electronic address. From there, the documents are automatically sent to the appropriate authorities for review. When the regulators have made their decisions, the decisions are communicated back to the importer or exporter through the same 'window' of communications.

Importers and exporters are subject to many regulations, depending on the goods (or more rarely services) that they bring or send across the border. The source of the regulations may be almost any government department. It is usually in the interests of efficiency that any communication between importers and exporters, on the one hand, and regulatory agencies, on the other, should be done electronically.

Making these communications electronic requires standardized format of information, i.e. forms, to be converted to electronic form. Ideally the forms would be machine-readable, to save on repeated data entry with its delay and its risk of error. Having these forms would facilitate the development of the Single Window. Many regulators are going electronic, and as the next subsection shows, the government is well aware of the advantages of harmonized or interoperable public services.

Here is what the Customs Authority advises importers are necessary documents to import:

> Business entities and individuals shall submit the following Customs documents when admitting goods and means of transport cross the state border:
> - Cargo Manifesto
> - Waybill or shipment documents
> - Foreign trade agreement
> - Pro-forma invoice
> - Product packaging documentation
> - Certificate of origin of goods
> - Permissions, licenses of related authorities (if required)
> - Product quality certificate, certificate of conformity, laboratory test results (if required)
> - Receipt of payment of customs taxes and related fees
> - Documents authorizing partial or complete exemptions from customs and other taxes (if necessary)
> - Customs declaration
> - Remittance for payment, price documentation

- Other materials on request [93]

The advantage of being able to lodge all of these in one place in electronic form is obvious… but such a system is not easy to build.

Documents proposing or planning a single (electronic) window for Mongolia to give access to all required approvals for import and export have been circulating since at least 2005,[94] but to date no such single window exists. A report for the Asian Development Bank in 2016 said it was complicated to build.[95] "… for the single window to become operative, establishing a legal framework is imperative."[96] Various partial initiatives were reported in 2021 by the World Trade Organization.[97] The (NTFC) 2022 Priorities report recommended the design of a single window.[98]

Normally a lead ministry builds a team of representatives from the main regulatory authorities within government, those that are called on to inspect or consider goods and services proposed for import (or export), along with private sector interests. The co-ordinating committee would ensure that everyone's capacities and interests are considering in building a system. Several committees have been created over the years. The NTFC is the current manifestation of the committee.

Normally as well, a statute is developed to ensure that the legal authority to participate and to collaborate in the single window system is clear. The contents of the statute and other interministerial agreements in support may be inspired by the CEFACT Guide to legal issues, noted below in the section about international standards.[99]

Our recommendation is in favour of legislation for the basic principles and permissions of a single window, though it may be supplemented by a network of contracts by which participants bind themselves to performance standards that may be enforceable by civil liability.

[93] Mongolia Trade Information portal, FAQs, online: https://mongoliatradeportal.gov.mn/index.php?r=site/display&id=5
[94] 2005 report https://www.adb.org/sites/default/files/project-document/68678/36027-03-reg-tacr.pdf
[95] ADB report, online: https://www.adb.org/sites/default/files/project-document/182730/47174-001-rrp.pdf para. 14.

[96] Footnote 95, para 16.
[97] WTO Trade Policy Review on Mongolia WTO/TPR/S/406 https://www.wto.org/english/tratop_e/tpr_e/s406_e.pdf
[98] Source?
[99] See text at footnote 171.

2. Electronic portal of public services

The government has been building an electronic portal by which Mongolian citizens and residents may communicate and transact with all levels of government. The Ministry of Digital Development and Communications now manages the program.

> The E-Mongolia system [was launched] on 1 October 2020. The main achievement is that today, it has become a large system that includes 656 services from 61 government organizations. In total, more than 12 million services have been provided online through this system. The system currently has 1.3 million users. That means one-third of the adult population uses the E-Mongolia platform. A total of 656 most demanded public services can be obtained from this system, from applying for a driver's license to applying for a passport. Features such as offering services based on customer behavior have recently been added.[100]

As noted earlier, communications from citizens can now be authenticated with a digital signature (private key and certificate) that is embedded in the citizen's national identity card.[101] There are other method of authentication as well, discussed under the Electronic Signature subsection above: a personal log-in system; communication through official state email; transmission of information through a shared system of official letter exchange; and – for document authentication – the use of a unique digital identifier in the document, issued by the unified system of state services. The unique identifier is mentioned in several laws referred to earlier.

One result of these e-government initiatives will probably be to familiarize people with the use of e-communications generally, with legal effect. It will make further private-sector uses more likely.

There is no e-government law so named, but a number of pieces of legislation were adopted together in late 2021, coming into force in May 2022, to support the various facets of the digital nation. They have been described as "fundamental laws of digital transformation":

> the fundamental laws of digital transformation have been approved by the Parliament of Mongolia in December 2021. These laws consist of Law on Public Information and

[100] "Mongolia to take digital development to a new level," Telecomm Review, 10 June 2022, online: https://www.telecomreviewasia.com/index.php/news/interviews/2791-mongolia-to-take-digital-development-to-a-new-level.

[101] Footnote 24 article 8.4. Non-citizens are also given means to use digital signatures but not through the national identity card, which they do not have. - article 10.

> Transparency, Law on Digital Signatures, Law on Cybersecurity, Law on Personal Data Protection.[102]

The lack of a detailed statutory framework is considered an advantage in flexibility:

> …the absence of any legal regulations gives us the opportunity to compete freely, think freely, and do our business freely. For example, we do not require any special license to run a start-up business based on new modern technologies. Others are free to do so, as long as they are not related in any way to the telecommunications business,
> ….
>
> [We] are working to build a legal framework for the creation of a tax-free zone for start-up businesses. If this law is passed, start-ups will pay a separate, smaller tax.[103]

A more detailed and illustrated description of the initiatives and their implications is found in a slide deck from UNCTAD on Mongolian initiatives.[104] It refers to several multi-year initiatives/plans as well.

From 2015 until this year, 2022, there was a national program known as Smart Government[105] based on legislation and operated chiefly by the Cabinet Secretariat. It had interlocking components covering much of the economy and society: capacity building, civil engagement, infrastructure, e-service delivery, innovation, open data and interoperability. The provision of government services directly to the population through the Internet was less the focus than the digitlization of the economy as a whole.

[102] Footnote 100. Emphasis added.
[103] Footnote 100. Designing such a tax system is discussed briefly later in this report, in part V.B.
[104] NTFC Global Forum 2022, https://unctad.org/system/files/non-official-document/GFS42-Davaa-TSENDSUREN.pdf. See also the Action Plan of The Government of Mongolia for 2020-2024, online: https://cabinet.gov.mn/wp-content/uploads/2020-2024_-ActionPlan_GOM_Eng_Edited_OE-2.pdf ; Mongolia's Five-Year Development Guidelines for 2021-2025, online: https://cabinet.gov.mn/wp-content/uploads/2020_FIVE_YEAR_DEVELOPMENT_GUIDELINE_OF_MONGOLIA_2021-2025_Final_OE.pdf ; Action Plan for 2021-2030 of Mongolia's Long-term Development Policy "Vision-2050“, online: https://cabinet.gov.mn/wp-content/uploads/Vision2050_-2021-2030_Activities_Final_OE.pdf ; and “Vision-2050” Long-term Development Policy of Mongolia, online: https://cabinet.gov.mn/wp-content/uploads/2050_VISION_LONG-TERM-DEVELOPMENT-POLICY.pdf

[105] Smart Government, online: https://www.smart.gov.mn/en/sub_1/

The Smart Government project has been succeeded by the Digital Nation[106] project, to run from 2022 to 2027.[107] The new program focuses on six goals: Digital infrastructure, e-Governance, Cybersecurity, Digital Literacy, Innovation and Production, and National Development Accelerator.[108] Again, it is being carried on in parallet with 'e-Mongolia' rather than incorporating it.

It is not clear that there is a need or a demand for additional special legislative or regulatory provisions about electronic government, or about government-to-citizen or government-to-government communications. The practice can be developed based on current laws and regulations.

C. The Customs Authority and Cross-border e-Commerce

In 2006, Mongolia joined the Revised Kyoto Convention on the Simplification and Harmonization of Customs Procedures. The main feature of the Convention is to have customs authorities apply a risk-based screen on imports. Shippers with good records and shipments of lower value may have their screening at the border expedited or done in bulk, to save time with an acceptably low probability of dishonesty or mistake that would cause loss of revenue. Such a system clearly represents the global best practice. Nonetheless Mongolia has not yet implemented the risk-based process.

Some countries' customs authorities have difficulty handling the volume of shipments that e-commerce can create, especially high volumes of relatively low-value packages. The ability to do so is largely a matter of assessing the risk of letting packages through without review. In Mongolia, this does not depend on legislative or regulatory reform at this point, since the Convention allows

[106] Digital Nation program, online (in Mongolian): https://mddc.gov.mn/wp-content/uploads/2022/07/%D0%9024-20220518-%D0%A6%D0%B0%D1%85%D0%B8%D0%BC-%D2%AF%D0%BD%D0%B4%D1%8D%D1%81%D1%82%D1%8D%D0%BD-%D0%B1%D0%B0%D1%80%D0%B8%D0%BC%D1%82%D0%BB%D0%B0%D1%85-%D1%87%D0%B8%D0%B3%D0%BB%D1%8D%D0%BB-%D0%B1%D0%B0%D1%82%D0%BB%D0%B0%D1%85-%D1%82%D1%83%D1%85%D0%B0%D0%B9_1658190818-1-1.pdf

[107] The program is described online: https://montsame.mn/en/read/302990

[108] Tara Neal, "Transforming Mongolia into a Digital Nation: Interview with the Ministry of Digital Development", online: https://www.thefastmode.com/expert-opinion/26849-transforming-mongolia-into-a-digital-nation-interview-with-ministry-of-digital-development

for this analysis. It is a matter of administration and technology. Mongolia is getting assistance from Switzerland and the WCO itself in administering its risk management activities.[109]

1. De minimis rules

Another way to reduce the crush of low-value packages that flow from e-commerce is simply to draw a line – a value – below which one simply ignores the packages. This is called a '*de minimis*" rule – essentially saying that packages below the threshold are not important enough to care about.[110]

The question becomes determining this value. Countries have a wide range of values that they care or do not care about, ranging from $1000 US to $100 or less. It is fair to say that most countries draw the line at $200 or less. There seems to be no principle behind any particular decision. Clearly the lower the value of the cutoff, the more packages may need to be inspected, which has an administrative cost – but which allows them to be charged duty to enter the country. On the other side, a high *de minimis* value reduces Customs' administrative burden and speeds the delivery of goods shipped in e-commerce, but it reduces the national revenue from tariffs.

Mongolia's rule at present is to exempt from duty (and thus inspection, except for security issues) an "Interstate postal parcel sent to an individual's name containing no more than two goods of the same type with a value not exceeding ten times the minimum wage for one month."[111] This amount is effectively the *de minimis* cutoff in Mongolia.[112]

---

[109] WCO, "Mongolia becomes part of the SECO-WCO Global Trade Facilitation Programme (GTFP) Family", July 2022, online:

http://www.wcoomd.org/en/media/newsroom/2022/july/mongolia-becomes-part-of-the-seco-wco-gtfp-family.aspx.

[110] The Latin expression was originally "de minimis non curat lex" – the law does not concern itself with trifles. Likewise Customs would not concern itself with low-value goods.

[111] Law on Customs Tariffs and Customs Taxes, art. 38.1.5, online: https://legalinfo.mn/mn/detail?lawId=208. See also the Law on Official Value Added Tax, article 13.1.24, with the same value cutoff – except for laptop computers, where the VAT begins at a value of 30 times the minimum wage for one month. Online: https://legalinfo.mn/mn/detail?lawId=11227.

[112] A full chapter on de minimis calculations is found in the ESCAP publication *Selected Issues in Cross-border e-Commerce Development in Asia and the Pacific.* Studies in Trade Investment and Innovation No. 21, 2019, online: https://www.unescap.org/publications/studies-trade-investment-and-innovation-no-91-selected-issues-cross-border-e-commerce.

a. Digression on Delivery

As noted, the *de minimis* rule in Mongolia applies only to items being sent through the postal system. This appears to have a harmful effect on competition and service levels for delivery of goods sold through e-commerce. In order for inexpensive foreign goods – a large volume of traffic - to enter tax-free, they must be sent by mail.

The government runs the post office, but the Law on the Post[113] has for several years allowed non-governmental businesses to get licences to deliver letters and goods as well. In practice, to benefit from the tax-free entry, delivery businesses must go to the trouble of being licensed under that Law. Most countries – China is a near-by example,[114] South Korea is another[115] - allow the duty exemption to apply to the goods themselves and not their delivery system, which allows for greater freedom of choice for shippers and less administrative engagement of carriers with the Post Office.

It may be worth a conversation between the responsible e-commerce ministries and the Ministry of Finance to see if the connection between the postal service and the tax-free status of shipments can be changed. Such a change would not normally change the amount of revenue produced by customs duties.[116]

2. Some examples of e-commerce systems

Creating the right mix of administrative rules and techniques to handle the demands of cross-border e-commerce can be a matter of trial and error. China has a very complex system, developed over many years. It used pilot projects as to types of good and experiments based on measures described in the ESCAP publication just mentioned.[117]

Vietnam has been addressing similar issues in deciding how its customs authority can respond to the volume of goods. For some time, the country had no special legal regime for e-commerce

[113] Law on the Post Office, online, https://legalinfo.mn/mn/detail/92
[114] In China, after ordering an item, the buyer may choose any available delivery service. China Post description, online: https://parcelsapp.com/en/carriers/china-post
[115] South Korea *Postal Service Act*, article 2(3), online: https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=55495&type=part&key=43
[116] At the workshop to discuss the draft of this report, held on 16 December 2022, it was reported that the procedure for customs clearance of interstate parcels approved by the Ministry of Foreign Affairs and the Ministry of Finance is in the process of being revised. No other information is available at this time.
[117] Footnote 112, pages 19 – 22.

and no separate track for the package, and it found itself overwhelmed by lack of approved tools. As a result, it prepared a Draft Decree on e-commerce administration.

> The Draft Decree introduces dedicated customs procedures for e-commerce transacted goods, including provisions on advance information submissions via a specialized customs electronic data processing system; exemptions from specialized management and inspection and from import tax; categorization of goods; and customs procedures for returned goods.[118]

To give an idea of the complexity of the issues once one comes to terms with them, however, it should be noted that the Draft Decree was issued in August 2021 and at the end of 2022, it remains a draft only. (The Draft Decree also proposes *de minimis* values for imports to Vietnam.)

The international best practices in the area are published by the World Customs Organization (WCO) in its recent document, *Framework of Standards on Cross-border e-Commerce.*[119] The first of the standards deals with the exchange of information on pending shipments before shipping, involving all parties to potential regulation of the goods in question:

> 2.1. Standard 1: Legal Framework for Advanced Electronic Data
>
> A legal and regulatory framework should be established for requiring advance electronic exchange of data between relevant parties involved in the E-Commerce supply chain, and Customs administrations and other relevant government agencies to enhance facilitation and control measures, taking into account applicable laws, inter alia, those related to competition (anti-trust), and data security, privacy, protection, ownership.[120]
>
> When establishing or adapting legislative frameworks for cross border E-Commerce, Governments should leverage, among others, existing WCO conventions, instruments

[118] Global Compliance News, October 2021, "Vietnam: Ministry of Finance releases draft decree on management of e-commerce transacted imports and exports," online: *https://www.globalcompliancenews.com/2021/10/14/vietnam-ministry-of-finance-releases-draft-decree-on-management-of-e-commerce-transacted-imports-and-exports061021/*
[119] Online: http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/activities-and-programmes/ecommerce/wco-framework-of-standards-on-crossborder-ecommerce_en.pdf?la=en (June 2022).
[120] Footnote 119, page 10. Standard 9 speaks of *de minimis* rules but says only that "Governments should make fully informed decisions based on specific national circumstances."

and tools, all relevant WTO agreements, in particular the Trade Facilitation Agreement (TFA) and other international conventions, standards and tools.[121]

The Mongolian Customs Authority is moving toward digital integration of its processes. This can be seen from its website. "Customs Electronic Service System."[122] It will need considerably more coordination and conversation to meet the WCO Standard. These conversations are happening, however. The procedure for customs clearance of interstate parcels approved by the Ministry of Foreign Affairs and the Ministry of Finance is in the process of being revised.[123] The Chinese and Vietnamese experience would not suggest that it will be quick or easy. Designing the Mongolian equivalent of Vietnam's Draft Decree is well beyond the scope of this report.

3. Intangibles

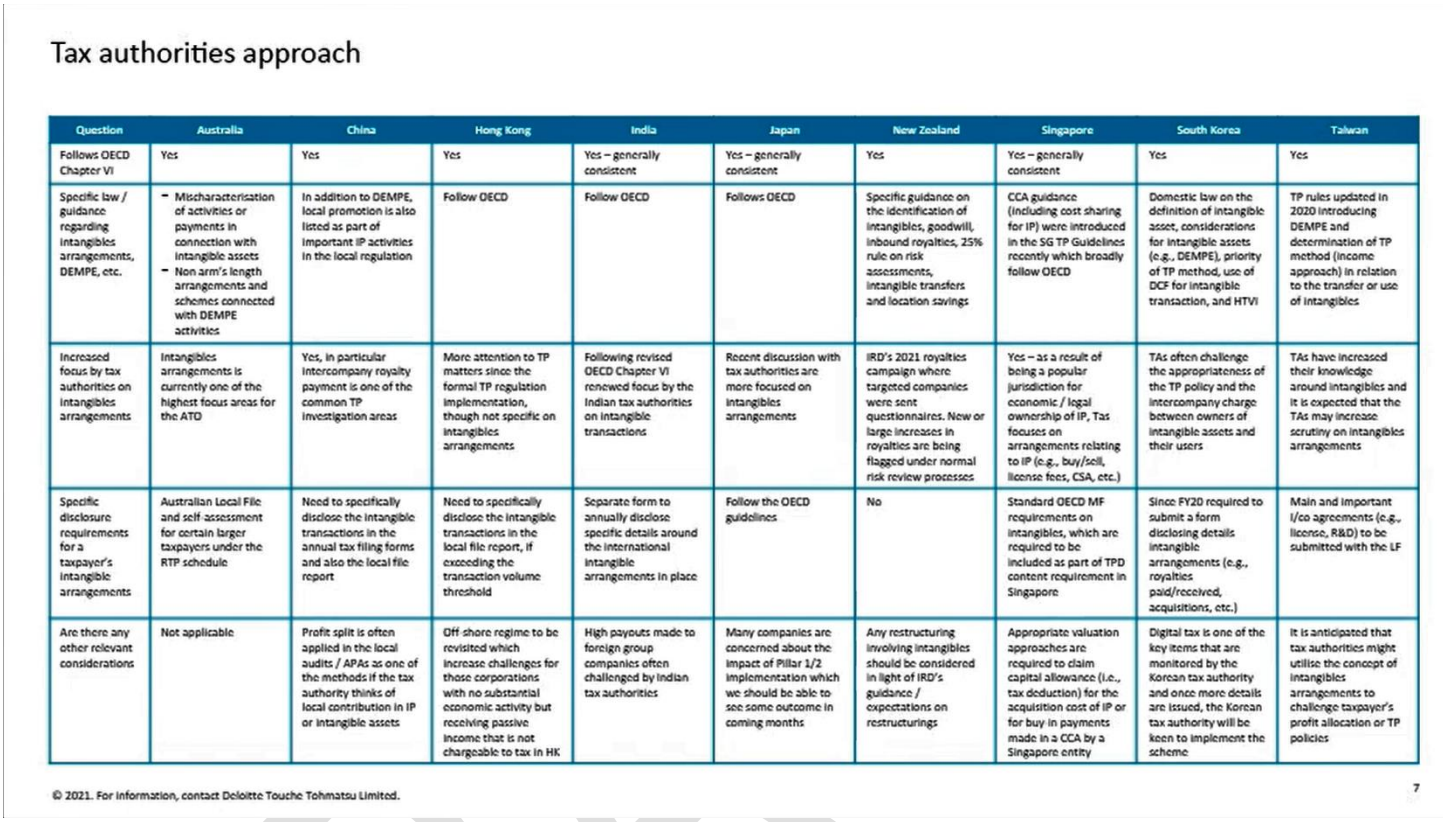
Traditionally customs matters have dealt with the value and regulation of the import and export of goods. Services tended to be provided on a personal basis, so if foreigners were going to provide them, they would need to come to their clients. At that point, their border issues were immigration matters, not customs matters, and their provision of services was subject to local law where they were provided.

The Internet has changed this. Many services can now be provided remotely, from anywhere in the world. Digital products may be developed and delivered electronically and undetectably by border officials. Intangible items may also be part of the value of goods shipped across borders as well, for example the value of intellectual property they represent (trademarks or patents). It may be that goods are to be used under a licence that produces a stream of revenue back to the foreign owner.

As a result, the focus of discussions has tended to move to transfer pricing. The WCO has a guide on the topic.[124] In addition, the Organization for Economic Cooperation and Development (OECD)

[121] Footnote 119, page 8. Some of the applicable international standards are reviewed in the next section of this report.
[122] Customs Electronic Service System, online: https://gaali.mn/
[123] Comment made in discussion session at the ADB workshop in Ulaanbaatar, 16 December 2022, on Legal and regulatory barriers to effective and efficient e-commerce in Mongolia.
[124] *WCO Guide to Customs Valuation and Transfer Pricing*, 2018, online: https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/key-issues/revenue-package/wco-guide-to-customs-valuation-and-transfer-pricing.pdf

has published principles that are widely recognized.[125] This "guidance" has been formally incorporated into the Transfer Pricing Guidelines as an annex to Chapter VI. Chapter VI on such intangible valuation forms the basis of the law of many Asian countries.[126]



Tax authorities approach

Question	Australia	China	Hong Kong	India	Japan	New Zealand	Singapore	South Korea	Taiwan
Follows OECD Chapter VI	Yes	Yes	Yes	Yes – generally consistent	Yes – generally consistent	Yes	Yes – generally consistent	Yes	Yes
Specific law / guidance regarding intangibles arrangements, DEMPE, etc.	– Mischaracterisation of activities or payments in connection with intangible assets – Non arm's length arrangements and schemes connected with DEMPE activities	In addition to DEMPE, local promotion is also listed as part of important IP activities in the local regulation	Follow OECD	Follow OECD	Follows OECD	Specific guidance on the identification of intangibles, goodwill, inbound royalties, 25% rule on risk assessments, intangible transfers and location savings	CCA guidance (including cost sharing for IP) were introduced in the SG TP Guidelines recently which broadly follow OECD	Domestic law on the definition of intangible asset, considerations for intangible assets (e.g., DEMPE), priority of TP method, use of DCF for intangible transaction, and HTVI	TP rules updated in 2020 introducing DEMPE and determination of TP method (income approach) in relation to the transfer or use of intangibles
Increased focus by tax authorities on intangibles arrangements	Intangibles arrangements is currently one of the highest focus areas for the ATO	Yes, in particular intercompany royalty payment is one of the common TP investigation areas	More attention to TP matters since the formal TP regulation implementation, though not specific on intangibles arrangements	Following revised OECD Chapter VI renewed focus by the Indian tax authorities on intangible transactions	Recent discussion with tax authorities are more focused on intangibles arrangements	IRD's 2021 royalties campaign where targeted companies were sent questionnaires. New or large increases in royalties are being flagged under normal risk review processes	Yes – as a result of being a popular jurisdiction for economic / legal ownership of IP, Tas focuses on arrangements relating to IP (e.g., buy/sell, license fees, CSA, etc.)	TAs often challenge the appropriateness of the TP policy and the intercompany charge between owners of intangible assets and their users	TAs have increased their knowledge around intangibles and it is expected that the TAs may increase scrutiny on intangibles arrangements
Specific disclosure requirements for a taxpayer's intangible arrangements	Australian Local File and self-assessment for certain larger taxpayers under the RTP schedule	Need to specifically disclose the intangible transactions in the annual tax filing forms and also the local file report	Need to specifically disclose the intangible transactions in the local file report, if exceeding the transaction volume threshold	Separate form to annually disclose specific details around the international intangible arrangements in place	Follow the OECD guidelines	No	Standard OECD MF requirements on intangibles, which are required to be included as part of TPD content requirement in Singapore	Since FY20 required to submit a form disclosing details intangible arrangements (e.g., royalties paid/received, acquisitions, etc.)	Main and important I/co agreements (e.g., license, R&D) to be submitted with the LF
Are there any other relevant considerations	Not applicable	Profit split is often applied in the local audits / APAs as one of the methods if the tax authority thinks of local contribution in IP or intangible assets	Off-shore regime to be revisited which increase challenges for those corporations with no substantial economic activity but receiving passive income that is not chargeable to tax in HK	High payouts made to foreign group companies often challenged by Indian tax authorities	Many companies are concerned about the impact of Pillar 1/2 implementation which we should be able to see some outcome in coming months	Any restructuring involving intangibles should be considered in light of IRD's guidance / expectations on restructurings	Appropriate valuation approaches are required to claim capital allowance (i.e., tax deduction) for the acquisition cost of IP or for buy in payments made in a CCA by a Singapore entity	Digital tax is one of the key items that are monitored by the Korean tax authority and once more details are issued, the Korean tax authority will be keen to implement the scheme	It is anticipated that tax authorities might utilise the concept of intangibles arrangements to challenge taxpayer's profit allocation or TP policies

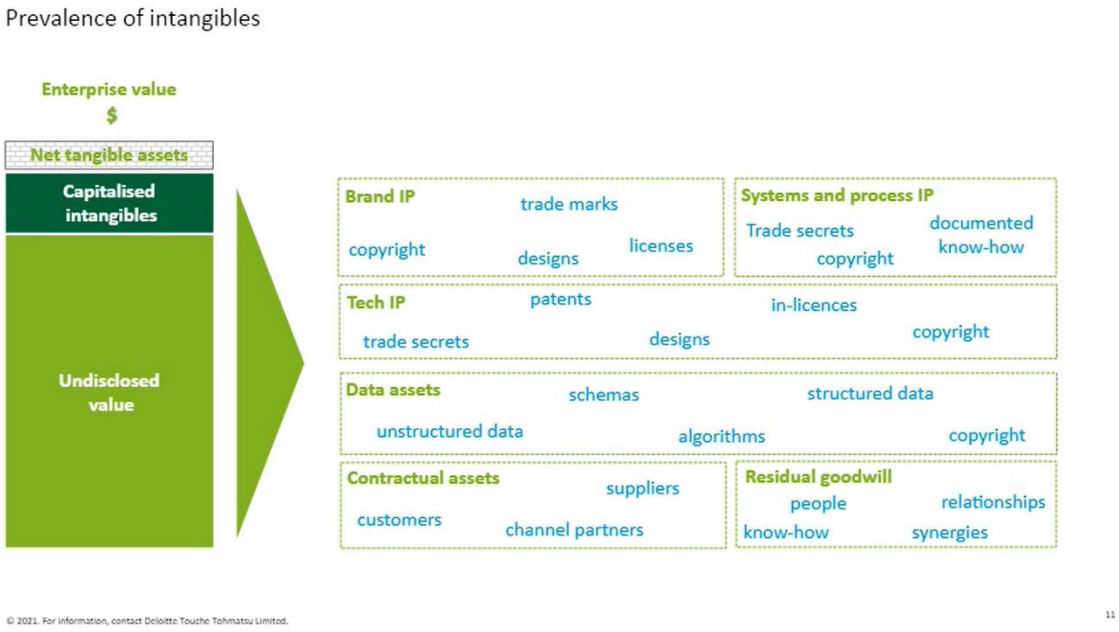
7

Here is an illustration of the kinds of intangible values that may arise in cross-border trade, including in e-commerce and sometimes especially in e-commerce:[127]

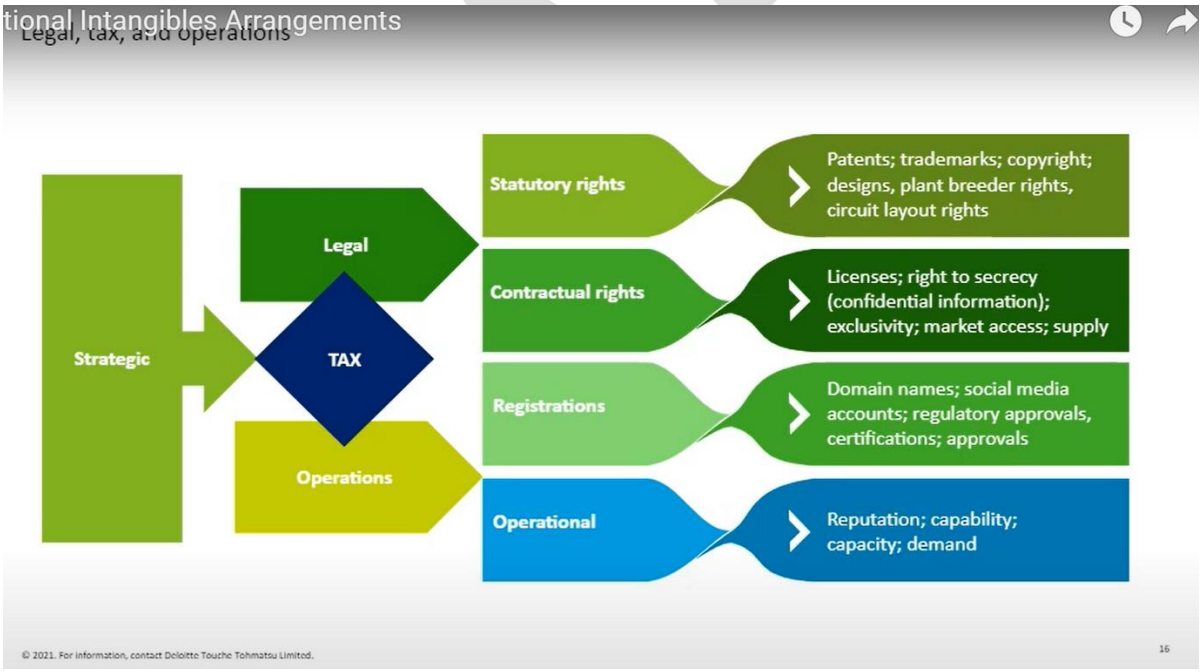
[125] *Guidance for Tax Administrations on the Application of the Approach to Hard-to-Value Intangibles - BEPS Action 8,* 2018, online*:* https://www.oecd.org/tax/transfer-pricing/guidance-for-tax-administrations-on-the-application-of-the-approach-to-hard-to-value-intangibles-beps-action-8.htm

[126] Deloitte, *Australia: ATO [Australian Taxation Office] guidance on International Intangibles Arrangements,* 18 November 2021, online: https://www.youtube.com/watch?v=YPG8_meiweQ&ab_channel=DeloitteDbriefsAP. See slide 7 at 13:33 for a chart of approaches of APEC member states.

[127] Deloitte, footnote 126 at 22:20



Finally, here is an indication of the legal and regulatory sources of the rights that will need to be arranged in e-commerce matters.[128]



[128] Deloitte, footnote 126, at 36:20.

It will be recognized that challenges of measuring trade in intangibles and in assigning a value to that trade for tax\customs purposes do not change the basic law of e-documents and e-signatures described earlier. The validity of a contract for intangibles, or partly for intangibles, is not affected by its content. Neither is its subjection to rules on consumer protection, privacy and the like, discussed later.[129]

4. Certificates of origin

The current Mongolian system among other things allows for electronic submission of customs declarations and scans of supporting documents.

One of the most important documents that accompanies goods imported or exported is a certificate of origin, attesting to the country where the goods, or a substantial part of their value, originated. This information allows Customs to know how to handle the goods and what level of duties to impose, if any. To be most effective, they should be developed in association with the country's main trading partners who will be called on to recognize them.

Customs processing can become much faster if such certificates are in digital form (and standard form). The Mongolian National Council of Chambers of Commerce and Industry (MNCCI) has the authority to issue these certificates. At present they are not being issued in electronic form.

IV. INTERNATIONAL FRAMEWORK: OBLIGATIONS AND POSSIBILITIES

Like other countries, Mongolia is party to a number of international commercial or trade agreements, and it could become party to others. Many of these either expressly authorize the use of e-communications or are expressed in media-neutral terms that would allow e-communications if those acting under the agreements (businesses or governments) chose to use them.

If the local laws tended to restrict e-communications, sometimes transacting parties could rely on the international agreements for their authority to go paperless. This is true in part because

[129] The validity of an international contract for services and the application of Mongolian laws will depend on private international law rules about whose law applies to the contract and the impact of mandatory local rules on it. Such an analysis is beyond the scope of this report.

Mongolian law routinely says that in the event of conflict between a national law and a treaty obligation, the treaty obligation prevails. It is also true in part simply because the international instrument may have a wider scope than the national one and leave more room for innovative practice across the border.

This is not so much a factor of concern today with Mongolia, whose policies favour such communications where possible, but international instruments may still fill gaps in policy permissions or offer flexibility in approaches to the use of ICTs.

In addition, some agreements are expressly about e-communications.

Moreover, one finds recognized international standards that can be used as the basis for e-communications technology, without the country having to join any body or agree legally to refer to the standards.[130]

A. Trade agreements that affect e-commerce

International free trade agreements have in the past decade begun including provisions to harmonize the legal regimes governing e-commerce in the participating countries. This has not been incidental or merely for facilitation; instead, these agreements explicitly promote reforms to commercial law to frame the legal effect of e-commerce. The World Economic Forum has reported that over half of the trade agreements currently in operation contain an e-commerce chapter which set out commitments to the facilitation of e-commerce.[131]

In some cases, the provisions aim only to bring the parties to a uniform level in their implementation of global standards. Such standards include the UN Commission on International Trade Law (UNCITRAL) model laws.[132] The provisions aim in other cases to compel parties to the trade agreements to adopt particular positions on controversial policies, such as a requirement

[130] Much of the explanatory text in this section is taken or slightly adapted from the principal author's report on CAREC E-commerce legislation published in 2021 by the ADB. *E-Commerce in CAREC Countries: Laws and Policies.* Online: https://www.adb.org/publications/e-commerce-carec-laws-policies.

[131] National Center for Asia-Pacific Cooperation, Working Group on E-Signatures, *Advancing Digital Transactions in APEC: Enhancing E-Signatures and digital Signatures,* March 2022, p 15. Online: https://ncapec.org/library/AdvancingDigitalTransactionsinAPECEnhancingE-SignaturesandDigitalSignatures.pdf. An alternative and perhaps more accurate formulation: more than half of WTO members have signed at least one [Regional Trade Agreement] that contain a standalone e-commerce provision. A. Darsinouei and R.Kakaub, "Understanding E-Commerce Issues in Trade Agreements", Geneva: CUTS International, 2017, 11. Online: https://www.cuts-geneva.org/pdf/STUDY%20-%20E-Commerce%20Towards%20MC11.pdf.

[132] Model Law on Electronic Commerce, footnote 18, and Model Law on Electronic Signatures, footnote 29.

that businesses should or should not locate data processing facilities in the country from which the data (particularly personal data) originate.

The phenomenon of pursuing paperless trade facilitation in recent international trade agreements was examined in 2017 by the Asian Development Bank (ADB) Institute, focusing on electronic trade facilitation rather than on legal reforms that apply to private transactions.[133] Other papers, including from the World Trade Organization, note several agreements with e-commerce provisions.[134]

Given differing legal and cultural traditions of the parties involved, trade obligations are often at a high level or are aspirational, making it difficult to support commercially effective legislation or resolve practical implementation issues. These provisions tend to state goals that the parties hope to somehow achieve one day but do not help to arrive at them.

Nevertheless, amid the heightened importance of digital trade and reinforced by the pandemic, trade agreements have emerged to the forefront of rule-making on digital trade issues. Notably, the Australia-Singapore Digital Economic Partnership Agreement,[135] the Digital Economy Partnership Agreement between Chile, New Zealand and Singapore[136] and the Comprehensive and Progressive Trans-Pacific Partnership,[137] aim to reduce trade barriers in the digital economy, build comparable standards, and promote regulatory harmonization in domestic legal frameworks governing electronic transactions and cross-border business.

Overall, if cross-border e-commerce is to deliver on its full potential, e-commerce issues must become an integral part of the trade policy agenda. There is an advantage to putting these provisions into trade agreements, since these agreements have a high public profile. These

[133] Duval, Y. and K. Mengjing. 2017. *Digital Trade Facilitation: Paperless Trade in Regional Trade Agreements*. ADBI Working Paper 747. Tokyo: Asian Development Bank Institute. Available online: https://www.adb.org/publications/digital-trade-facilitation-paperless-trade-regional-trade-agreements.
[134] Monteiro, José-Antonio & Teh, Robert, 2017. "*Provisions on electronic commerce in regional trade agreements*", WTO Staff Working Papers ERSD-2017-11, World Trade Organization (WTO), Economic Research and Statistics Division, online https://ideas.repec.org/p/zbw/wtowps/ersd201711.html.
[135] Online: https://wits.worldbank.org/GPTAD/PDF/archive/Singapore-Australia.pdf
[136] An overview with link to the official text are online: https://www.mti.gov.sg/Improving-Trade/Digital-Economy-Agreements/The-Digital-Economy-Partnership-Agreement
[137] Online: https://www.dfat.gov.au/trade/agreements/in-force/cptpp/official-documents

provisions can attract political attention in a way that technical law reform rarely does, which can generate the political will to implement them in domestic law. [138]

1. Now in force in Mongolia

a. The World Trade Organization Trade Facilitation Agreement[139] requires contracting states to use e-communications for a number of domestic and international purposes. Parties are given time to comply with the requirements, depending on their state of economic development.

It is worth noting that the WTO obligations include technology neutrality where possible.

Mongolia has been a party to the WTO TFA since 2016. As a country classified as a developing economy, it has currently met just over 75% of its obligations to use paperless communications.[140] The delay, if any, is technological - putting the systems in place – rather than legal, since the TFA itself provides the legal authority.

b. Revised Kyoto Convention (World Customs Organization's International Convention on the Simplification and Harmonization of Customs Procedures (as amended)). Mongolia joined this convention in 2006.

The 2006 revision changed customs practice from inspecting every package to managing the risk of contraband and other unsuitable goods, and promoted the use of electronic forms.[141] The 2022 report of the WTO acknowledges this agenda and supports Mongolia's capacity to carry it forward.[142]

---

[138] J.D. Gregory, "Trade Agreements to Promote Electronic Commerce", Slaw.ca blog: part I, 2016, online: http://www.slaw.ca/?s=trade+agreements+electronic+commerce ; part II, 2018, online: http://www.slaw.ca/2018/11/08/trade-agreements-to-promote-electronic-commerce-ii/; part III, 2019: http://www.slaw.ca/2019/12/30/trade-agreements-to-promote-electronic-commerce-iii/.

[139] World Trade Organization, Trade Facilitation Agreement, online: https://www.wto.org/english/tratop_e/tradfa_e/tradfa_e.htm

[140] See the WTO table of progress in implementation, online: https://tfadatabase.org/implementation/progress-by-member and https://tfadatabase.org/en/members/mongolia.

[141] The Revised Kyoto Convention is described here: http://tfig.unece.org/contents/revised-kyoto-convention.htm. A guide to its provisions is here: https://www.wcoesarocb.org/wp-content/uploads/2018/07/1.-WCO-Revised-Kyoto-Convention.pdf

[142] WCO, "Mongolia becomes part of the SECO-WCO Global Trade Facilitation Programme (GTFP) Family", online: http://www.wcoomd.org/en/media/newsroom/2022/july/mongolia-becomes-part-of-the-seco-wco-gtfp-family.aspx

c. UN/ESCAP Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific [143]

The agreement sets out principles of a rational, acceptable, harmonized approach to cross-border paperless trade. It encourages parties to the agreement to create a national policy on this trade, establish a single window to handle documentation destined for different agencies within the state, and set up systems to promote the mutual recognition of trade documents among member states (and other trading partners). Each contracting party is to take these steps, which all align with international best practices, in ways consistent with its own legal system and traditions.

The framework agreement encourages rather than requires actions, which allows ESCAP member states such as Mongolia to join no matter how ready they currently are to engage in cross-border paperless trade. The rules serve as guides for those at the early stages, and as confirmation of steps already taken for those more advanced in the process. They provide a route along which all the parties can work in a consistent way (but at their own pace) to facilitate their trade with each other and the rest of the world. ESCAP may also be able to offer resources to help parties to the agreement engage in cross-border paperless trade.

d. Mongolia-Japan Free Trade Agreement

Mongolia and Japan have made a free trade agreement, called an "economic partnership", as of 2016.[144] It has a full chapter on electronic commerce largely consistent with the state of the international art. That chapter starts out with a declaration that the parties "recognize the principle of technological neutrality in electronic commerce." (Article 9.1(3)

It defines electronic signature as a measure applied to an e-record that indicates that the information in the record has been approved by the person taking the measure and that confirms that the information has not been altered. The latter function is usually associated with a digital signature, based on the use of a hash function described earlier in this report.

Nonetheless article 9.5 of the agreement says that the parties shall not adopt or maintain measures about e-signatures that would "prohibit parties to an electronic transaction from

[143] Sources of information on the Framework Agreement are online: https://www.unescap.org/kp/cpta
[144] Agreement between Japan and Mongolia for an Economic Partnership, online: https://www.mofa.go.jp/policy/economy/fta/mongolia.html.

mutually determining the appropriate electronic signature methods for their transaction." Are transacting parties therefore to be free to choose e-signatures less onerous and less regulated than digital signatures?

Whether the provisions of the Law on Electronic Signatures that promote the use of digital signatures are contrary to this agreement is a complex question. That Law does promote their use but does not require them. Alternative forms of authentication exist, as discussed earlier. Moreover, that Law says in article 2.2 that if an international treaty to which Mongolia is a party provides otherwise than this law, the provisions of the international treaty shall prevail. So it is likely that parties to a transaction between Mongolia and Japan would have the flexibility of the free trade agreement.

B. Regional economic cooperation agreements

Agreements about regional economic cooperation may require the participating states to take legislative measures to express the cooperation, including in trade matters. They can be important in any event to the expansion of e-commerce among the parties, by allowing for discussions of matters of common interest, such as rules for cross-border flows of personal or economic information, cooperation in fighting cybercrime, and the like.

1. Now in force in Mongolia

a. Central Asia Regional Economic Cooperation (CAREC)

The CAREC Program unites eleven central Asian countries to promote regional development, notably in transportation, energy, and poverty reduction.[145] It has not engaged in notable work on electronic commerce, beyond publishing (with the ADB) a study in 2021 on e-commerce laws and regulation,[146] and very recently, a review of the technological infrastructure for e-commerce in member states.[147] Efforts to develop or harmonize those laws or that regulation have not

[145] Central Asia Regional Economic Cooperation, online: https://www.carecprogram.org/
[146] J. Gregory, *E-Commerce in CAREC Countries: Laws and Policies*, ADB 2021, footnote 109.
[147] Footnote 4.

followed, at least not co-ordinated or led by CAREC, though CAREC does have a digitalization agenda[148].

2. Potential regional trade agreements for Mongolia

a. Regional Comprehensive Economic Partnership[149]

The RCEP is a creature of the Asia-Pacific Economic Cooperation (APEC) organization that includes most significant Asian economies, including the People's Republic of China, the Republic of Korea, Japan, Singapore and Australia. It came into force on 1 January 2022 and is open for accession by any other "state or unit" in the region for 18 months.[150] The official text does not say what "the region" is for this purpose, but it is reasonable to assume that any Asian nation would be welcome, especially one bordering a member state – in Mongolia's case, China.

While the RCEP does reduce tariff barriers among its members, it also contains a chapter on electronic commerce law and regulation.[151] Most of the chapter is in terms of "the parties shall endeavour" to achieve cooperation and harmonization in their laws and practices of e-commerce. They are obliged to have a legal framework "taking into account" the UNCITRAL Model Law on Electronic Commerce and the UN Electronic Communications Convention, and other model laws and international conventions relating to e-commerce. (article 12.10) They must also adopt recognized principles for consumer protection (12.7), privacy protection (12.8) and fighting unsolicited commercial messages (spam)(12.9). These provisions also stress enforcement of the rights given.

The rules on electronic signatures are as strong as any rule in RCEP (article 12.6).

> Except in circumstances otherwise provided for under its laws and regulations, a Party shall not deny the legal validity of a signature solely on the basis that the signature is in electronic form.

[148] *CAREC Digital Strategy 2030,* online: https://www.carecprogram.org/?page_id=18952
[149] Source materials on the Regional Comprehensive Economic Partnership (RCEP) are online: https://rcepsec.org/. The legal text is online: https://rcepsec.org/legal-text/.
[150] RCEP, legal text, footnote 152, article 20.
[151] RCEP, footnote 152, chapter 12, Electronic Commerce, online : https://rcepsec.org/wp-content/uploads/2020/11/Chapter-12.pdf

> Taking into account international norms for electronic authentication, each Party shall:
> (a) permit participants in electronic transactions to determine appropriate electronic authentication technologies and implementation models for their electronic transactions;
> (b) not limit the recognition of electronic authentication technologies and implementation models for electronic transactions; and
> (c) permit participants in electronic transactions to have the opportunity to prove that their electronic transactions comply with its laws and regulations with respect to electronic authentication.

However, some performance standards may be imposed on some kinds of signature under some circumstances (article 12.6(3)). In fact, most obligations in RCEP are subject to discussion or consultation based on overriding public interests in the member states, and rules or prohibitions turn out to be less absolute than their framing appears as a first impression.

In short, RCEP may give to Mongolia some allies in developing e-commerce practices, but probably its best use for e-commerce is in providing links for cross-border cooperation in enforcing rules on parties from outside the country.

C. Instruments that expressly target e-commerce for its own sake

1. E-Commerce instruments now in force in Mongolia

a. United Nations Convention on the Use of Electronic Communications in International Contracts (the E-Communications Convention or ECC)**.** This convention was acceded to by Mongolia in May of 2020 and came into force on July 1, 2021.[152]

This Convention restates many of the rules for e-communications in the UNCITRAL Model Laws on Electronic Commerce and Electronic Signatures. A memorandum to the Mongolian Cabinet points out some of the gaps in Mongolian law that the ECC will help to fill:

> These legal provisions [in the Civil Code, mentioned in the first section of this report] did not define a legal status of electronic documents and did not recognize electronic

[152] The UNCITRAL press release about the accession is online: https://unis.unvienna.org/unis/en/pressrels/2020/unisl309.html

documents equally with paper-based documents while e-mails, computer files, short-letter messages (sms) on mobile phones and electronic data of databases are not clearly defined as a legally capable evidence material.[153]

Article 20, para 2 of the Convention provides a method by which a contracting state may interpret other international commercial conventions to which it is a party, in the light of UNCITRAL's e-commerce principles. This avoids the need to have these conventions modified expressly to allow e-communications. This could extend the benefits of such communications to many legal international relationships of Mongolia.[154] The New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards and the UN Convention on the International Sale of Goods are two examples mentioned in the Cabinet memorandum.

b. Customs Convention on the International Transport of Goods under Cover of TIR Carnets (TIR Convention) with Annex 11 on digital documents (in force May 2021).[155] Annex 11 appears to come into force automatically, i.e. member states of the Convention do not have to take separate legislative action to have it apply. The Convention harmonizes the documents needed to have commercial road traffic cross borders easily.

2. Potential instruments on electronic communications

a. WTO Joint Initiative on Electronic Commerce[156] A substantial number of members of the WTO began discussions in 2017 on facilitating e-commerce among themselves, beyond the provisions of the TFA already mentioned above. These discussions continue, in different formats and in different places. Mongolia participates in them though has not yet made any formal submission or proposal to the group.

---

[153] Cabinet document, "PRESENTATION OF THE DRAFT LAW ON RATIFICATION OF THE UNITED NATIONS CONVENTION ON USE OF ELECTRONIC COMMUNICATIONS IN INTERNATIONAL CONTRACTS" (translated for this report from "ОЛОН УЛСЫН ЭРЭЭНД ЦАХИМ ХАРИЛЦААГ АШИГЛАХ ТУХАЙ НЭГДСЭН ҮНДЭСТНИЙ АЙГУУЛЛАГЫН ОНВЕНЦЫГ СОЁРХОН БАТЛАХ ТУХАЙ ХУУЛИЙН төслийн ТАНИЛЦУУЛГА") [**source?]**

[154] There is also a respectable argument for harmonizing one's domestic e-commerce law with the ECC, to make all transactions on an equal legal footing. Singapore and Australia have done this, and it has been recommended for Canada.

[155] UN/ESCAP, Towards Electronic TIR Customs Transit System (eTIR), September 2014, online: https://www.unescap.org/sites/default/d8files/knowledge-products/brief12.pdf.

[156] WTO, *Joint Initiative on e-Commerce*, online: https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm

> The issues raised in members' submissions are discussed under six main themes: enabling electronic commerce, openness and electronic commerce, trust and digital trade, cross-cutting issues, telecommunications, and market access.[157]

The most recent meeting, in October 2022, hoped for a revised negotiating text by the end of the year.[158] If an internationally accepted text is produced, which is likely to be still some years away, it could have a very important role in harmonizing e-commerce laws at a deeper level than we have seen before. In sum, this instrument would be more significant than the following items, but they have the merit of being available for implementation now.

b. UNCITRAL Model Laws on Electronic Commerce and Electronic Signatures. [159]

These model laws represent the international state of the art for removing legal barriers to electronic commerce. Some parts of the former are arguably rendered unnecessary by the Civil Code provisions allowing for electronic documents. The latter is overtaken, or at least shadowed, by the Mongolian Law on Electronic Signatures. Their operation has been discussed in more detail earlier in this report.

c. UNCITRAL Model Law on Electronic Transferable Records

Adopted in 2017, the Model Law on Electronic Transferable Records provides an electronic functional equivalent to important trade documents that themselves suffice to transfer the value of the goods they describe.[160] Examples are bills of lading and warehouse receipts. Possession of the document entitles the holder to possession of the goods, so there should be only one document giving this right for any set of goods. This Model Law overcomes difficulties in creating unique electronic records, relying on appropriate assurances (not just in words but in technology) that an authoritative version of the record exists and can be safely transferred electronically. The MLETR is in early stages of implementation around the world but should be kept in mind in a comprehensive e-commerce legislative strategy.

---

[157] Footnote 159, under title "How are the e-commerce JI negotiations conducted?

[158] The report of that meeting is online: https://www.wto.org/english/news_e/news22_e/ecom_28oct22_e.htm

[159] Footnotes 18 and 29 above.

[160] Model Law on Electronic Transferable Records, 2017, online: https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records

D. Other current treaties and related agreements

1. Treaties now in force in Mongolia

a. Convention on the International Sale of Goods (CISG)

This convention, sometimes known as the Vienna Sales Convention, sets basic rules for the sale of goods between parties in different states. It was adopted in 1980 and does not expressly authorize electronic communications. However, the UN Convention on Contracts for the International Sale of Goods Advisory Council, a private group of experts on sales law, has found the convention to be consistent with electronic communications and to operate in the same way when they are used.[161] As noted above, for greater certainty, a declaration could be made about the CISG under the EEC.

This could have important consequences for countries like Mongolia that are parties to the CISG, since the Convention applies automatically to international sales contracts unless the contracting parties opt out. In other words, the law mandatorily applicable to such contracts permits e-communications to make them. This could provide useful flexibility to businesses looking to do international sales with e-documents, especially in countries where international treaties prevail over domestic laws, which include most of the CAREC members.

b. Sanitary and Phytosanitary (SPS) Agreement

There are several treaties on the trade in plants, notably the International Plant Protection Convention (IPPC) from the World Food Organization (FAO) dating from 1951, and a World Trade Organization SPS agreement that interacts with the IPPC.[162] Mongolia joined the IPPC in 2009. The current versions allow or contemplate the exchange of information electronically. In particular,

[161] UN Convention on Contracts for the International Sale of Goods-Advisory Council Opinion no. 1, Electronic Communications under CISG, 15 August 2003. http://www.cisgac.com/cisgac-opinion-no1/.
[162] Technically the WTO agreement is part of the general membership of WTO, rather than separate. It may, however, help to focus attention on specific areas of activity on which progress can be made incrementally.

National Notification Authorities may now use the SPS Notification Submission System (SPS NSS) to fill out and submit SPS notifications.[163]

c. Convention on Trade in Endangered Species (CITES)

The United Nations (UN) Convention on Trade in Endangered Species allows for electronic declarations of exemptions from trade bans using electronic forms.[164] Mongolia became a member in1996.

d. United Nations International Convention on the Harmonization of Frontier Controls of Goods

This convention allows standard reference to products in trade, which makes standard forms and thus electronically readable documents easier.[165] Mongolia became a party in 2007.

e. United Nations Layout Key for Trade Documents

The UN Layout Key is a document – not itself a convention - used in conjunction with the UN convention (footnote 137) to enable readers to understand forms even when the forms are prepared in a language that they do not comprehend.[166] The forms speak for themselves once they are standardized. The United Nations International Convention on the Harmonization of Frontier Controls of Goods makes the use of this layout mandatory for member states. The UN Centre for Trade Facilitation and Electronic Business (UNE/CEFACT) says that the Layout Key "can also be used to design screen layouts for the visual display of electronic documents."[167]

[163] See WTO web pages for information: https://www.wto.org/english/thewto_e/coher_e/wto_ippc_e.htm and https://www.wto.org/english/tratop_e/sps_e/sps_e.htm.

[164] Convention on International Trade in Endangered Species of Wild Fauna and Flora. 1973 (amended 1979 and 1983). Convention text. https://cites.org/eng/disc/text.php. See also https://cites.org/eng/disc/what.php for a description of the Convention.

[165] A description is here: http://tfig.unece.org/contents/Harmonized-frontier-controls-convention.htm and the text here: http://www.unece.org/fileadmin/DAM/trans/conventn/ECE-TRANS-55r2e.pdf

[166] http://tfig.unece.org/contents/recommendation-1.htm

[167] See the description of Recommendation 1 at: http://www.unece.org/tradewelcome/un-centre-for-trade-facilitation-and-e-business-uncefact/outputs/cefactrecommendationsrec-index/trade-facilitation-recommendations.html

E. International standards

1. Now available

a. UN Centre for Trade Facilitation (CEFACT) recommendations

These documents are not mandatory, as are conventions, but they provide internationally approved best practices for implementing workable rules or electronic trading. Its texts on the legal and administrative considerations in establishing a Single Window were mentioned above, as was the harmonized layout document. There is a large and useful collection of trade facilitation standards, some of them focused on the law, grouped as recommendations.[168]

b. International Standards Organization (ISO) standards

ISO standards have many applications for approaches to cross-border e-commerce. Among the most important are those affecting authentication certificates and information security - the 27000 series.[169]

c. Internet Standards

The Internet Engineering Task Force (IETF)[170] has created over the past half century a number of vital standards to express the design of the Internet and to keep it running. An important standard for digital signatures is the digital certificate, standard X.509.[171] Technical designs in Mongolia would be expected to follow these standards.

V. FRAMEWORK AND CONTEXT FOR ELECTRONIC COMMERCE[172]

Mongolia has been actively reviewing its laws concerning electronic communications, both in commercial matters and in the relations between state and citizen. Some laws are very recent: the *Law on electronic signatures* dates from December 2021 and came into force in May 2022. The *Law on consumer protection* is likely to be overhauled by early 2023. Some implementing

[168] UNE/CEFACT Recommendations on Trade Facilitation, online : https://unece.org/trade/uncefact/tf_recommendations
[169] International Standards Organization, ISO/IEC 27001 Information Security Management, online: https://www.iso.org/isoiec-27001-information-security.html
[170] Internet Engineeering Task Force, online: https://www.ietf.org/
[171] The X.509 digital certificate standard, online: https://www.ssl.com/faqs/what-is-an-x-509-certificate/
[172] Much of the explanatory text in this section is taken or slightly adapted from the principal author's report on CAREC E-commerce legislation published in 2021 by the ADB. Footnote 130.
John Gregory and Delgermaa Anbat

regulations for other laws are likewise quite new and untested. The UN Electronic Communications Convention came into force for Mongolia in July 2021. The UN/ESCAP Framework Agreement on the Facilitation of Cross-border Paperless Trade in Asia and the Pacific was acceded to effective in July 2022.

To appreciate the impact of these considerations on the Mongolian economy and in particular on the legal framework for economic activity, the report reviews principles of regulation and the legal best practices for electronic transactions and several particular aspects of them. This will prepare the way for recommendations for law reform in the following section.

Principles of Regulation

The section on Electronic Transactions at the beginning of this report reviewed UNCITRAL's work aimed to enable electronic transactions in a world full of requirements designed for paper documents. While the work was useful, as shown by its widespread adoption around the world, it did not claim to be everything a legal system would need in order to support electronic communications. UNCITRAL's silence on regulatory matters was not an assent to existing rules or a statement that nothing more was needed to facilitate electronic commerce.[173]

It has become clear, if it was not always clear, that the successful spread of electronic commerce in a society depends on a number of factors. The technology has to be available, the means to generate, receive and transact with electronic documents. The best enabling law will not build a computer where none exists or teach someone to use it once built. The host economy has to be rich enough and vibrant enough to support innovation, since some attempts to launch e-businesses will fail.

Another very important, though intangible, factor is that people must be willing to trust e-commerce: the technology and the people. Is it too risky to venture onto a computer, onto the Internet? Who and what is out there?

Trust has many facets. It is a kind of judgment about future conduct. In a trustworthy society, people keep their word, fulfil their contracts, act properly, because that conduct is expected. If this is not so in the physical economy – if people are fearful to engage in transactions with strangers

[173] See Guide to Enactment, MLEC, footnote 18, paragraphs 13 - 14

– then it may be even more difficult online, where one cannot see the people one is asked to deal with.

On the other hand, some measures of cybersecurity can make electronic transactions more trustworthy than dealings in person. E-commerce transactions may be more transparent and auditable than traditional in-person interactions. This is a trustworthiness that needs to be demonstrated and learned, however.

Recently the Asian Development Bank and the United Nations Economic and Social Commission for Asia and the Pacific (UN/ESCAP) published a study of the spread of e-commerce in Asia.[174] They observed that the development of e-commerce depended on economic factors and conditions, the legal and institutional environment, and social acceptance and awareness.[175] These three dimensions were inter-related; they all affected each other, and it was hard to arrive at mature e-commerce in society without all three being in good shape.

It is beyond the scope of this report to evaluate Mongolia's state of economic development or degree of social trust. However, there are legal measures besides UNCITRAL's enabling of electronic transactions that can build economic trust, that can make e-commerce appear safer and more appealing to potential businesspeople and their potential customers. The ADB/ESCAP study and several others[176] consistently mention the legal and institutional framework of e-commerce, and the consistent content of that framework includes rules of consumer protection, privacy, and online security, i.e., protection against online crime. These are crucial elements of trust and thus of growing e-commerce.[177]

A useful overview of principles, particularly but not solely devoted to consumer protection in e-commerce, was published in 2021 by US AID: *E-Commerce Code of Conduct: Recommendations*

[174] *Embracing the e-Commerce Revolution in Asia and the Pacific,* June 2018, footnote 5. The document includes examples from several CAREC member states.

[175] Footnote 5, p. 13.
[176] For example, see UNCTAD, *Rapid e-Trade Readiness Assessments of Least Developed Countries: Policy Impact and Way*, (2019), online: https://unctad.org/en/PublicationsLibrary/dtlstict2019d7_en.pdf;
UN/ESCAP, *Digital and Sustainable Trade Facilitation: Global Report* 2019, online: https://untfsurvey.org/report.
[177] That said, laws to remove legal barriers to the use of e-communications can also be seen as building trust, especially where the law touches on authentication. See John D. Gregory, "Legislating Trust" (2014), 12 *Canadian Journal of Law and Technology* No.1, 1. Online: https://digitalcommons.schulichlaw.dal.ca/cjlt/vol12/iss1/1/

for e-commerce development in Central Asia.[178] Its contents are consistent with the rest of the present report.

A. A law on electronic commerce

The first element of a legal framework for electronic commerce is a law about electronic commerce itself. While the basic electronic commercial transaction – buying and selling – is valid today, the Civil Code leaves a lot of questions unanswered. Some of them were mentioned by Cabinet in proposing accession to the E-Communications Convention: the status of messages that are not contracts, the timing of messages, admissibility of electronic evidence. The general interchangeability of media of communications – so information can be legally effective if conveyed through a tangible or an intangible medium – is worth saying in law.

A good way to create that effect would be to implement the E-Communications Convention for domestic law. The ECC has most of the important provisions of the Model Law on Electronic Commerce and the basics of the Model Law on Electronic Signature. If one were implementing the Model Laws instead of the ECC, then the MLEC is arguably the more important to enact, since Mongolia has no equivalent legal rules. Mongolia already has its Law on electronic signatures, but revisions to it would also be useful, as noted earlier. Adopting the ECC allows to focus on both at the same time.

Since Mongolia does not have a generic e-commerce law, using the Convention's language would not be difficult. The main challenge might arise because the legal effectiveness of an electronic document would not depend on its being duly signed, as with the Civil Code, but on its permanence, or at least "accessibility for subsequent reference".[179] However, it is likely to be acceptable to allow transactions to depend on signature but the general validity to depend on permanence for its purpose. ("Subsequent reference" does not have to mean "forever", any more than a document on paper has reduced legal effect because the paper could be destroyed. Record retention rules are separate from stability of the medium and have their own provision in the UNCITRAL texts.[180])

[178] US AID, 2021. Copy in possession of the authors.
[179] ECC footnote 19 article 9.2
[180] The records retention rule could be imported from the Model Law on Electronic Commerce, article 10. The ECC having been prepared for international trade, it does not deal with retention of records, a more domestic law concern.

The E-Communications Convention has a number of provisions about electronic signatures. This report has analysed the Law on Electronic Signatures and some of the potential for improving it, in an earlier section. It is mentioned here for the sake of completeness in a review of new e-commerce/e-signature laws in their broader context. Any domestic version of the ECC should of course be consistent with the law of e-signatures, even if the latter continues to be a free-standing statute and not rolled into the e-commerce law.

The other possible contents of such a "framework" statute are the points raised by stakeholders in the June 2022 workshop, as described in section 1.D of this report. On review, they do not focus much on validity or use of e-communications but on regulation and fairness. They can fit into a law alongside the ECC provisions without much difficulty.[181]

B. An e-commerce business

An electronic commerce statute can apply to any commercial transaction carried out by anyone by electronic means. However, there may be reasons of public policy to care who is doing the transactions and under what circumstances.

One of the reasons is visibility: governments have a statistical interest in knowing what economic activity is being carried on, in part as managers of the national economy, in part as controllers of taxation – both as a source of state revenue and as actors who might be encouraged to act in ways that benefit public policies such as high employment, innovation and trade. Business registration rules can go some way to creating visibility, if the registration asks registrants about the type of their business.

It is possible to describe a business with more permanence or more economic impact and give it its own legal category. For example, the draft Law on consumer protection defines the class of "e-business operator" as "an entrepreneur – a manufacturer of goods or seller of goods or services – who offers products and services through his official website and concludes a contract". So just doing business through one's own website, and not, for example, through a trading platform or through a Facebook page, would qualify a person or entity as such an operator, and such a business.

[181] The international consultant on the present report wrote a brief document on implementing the ECC for domestic purposes, for the CAREC Institute in 2020. It is attached as an appendix to this report]

Websites make a business visible. Visibility will attract taxation. However, individuals or small organizations might not want to register if it exposes them to taxes – including social charges to support worker benefits and other social programs. (Registration is often not optional for any business. The question here is whether to identify oneself as an e-commerce enterprise – again, if one has the choice in law. At present, the situation in Mongolia is not completely clear – hence this discussion.)

One way to increase the number of businesses registering is to offer some advantage for doing so: a lower tax rate for electronic sales, for example. Only businesses that register as e-commerce businesses might be allowed to receive the payment/subsidy.

Thus operations will self-identify as e-commerce businesses. The others, smaller or individual sellers, perhaps operating through a page on Facebook or Instagram, still have the benefit of statutory validation of their contracts, they are still subject to tax on their income in the normal way, they still have obligations to consumers, but they would be less important for public policy purposes.[182] (Operations run from Facebook are not necessarily small, certainly not necessarily smaller than some bricks-and-mortar businesses. One can consider questions of formality or structure as one possible criterion.)

Another way to distinguish the "serious" businesses that one might want to regulate, or benefit with special tax rates, would be by volume of sales, an objective measurement if one can count on honest reporting. Would the regulatory purpose of identifying e-commerce businesses vary with the size of the business, so that drawing a line based on sales would help?

More traditional physical evidence may have a role to play. The state may decide it cares more about businesses with physical locations outside the sole operator's residence, ones with offices or factories or shops and employees.

In any event one would need to decide what proportion of a business must be carried out electronically before it counts as an electronic business. The answer to that may depend on why one wants to know: estimating bandwidth required for a communications system might be different from estimating the revenue from kinds of business taxes.

[182] One may compare the scope of the Chinese Law on Electronic Commerce, described below, text accompanying footnote 190.

Here is an example of the sides of a debate on whether one should distinguish between the kinds of online businesses that might benefit from state support.

1. In favour of treating all online businesses the same: There is no need for a difference in treatment between one kind of e-commerce seller and another. If the state wants to encourage e-commerce, the reasons for doing so apply to any form of such commerce. The only useful distinction is volume and variety of products. The same basic law should apply to everyone. They should pay taxes at the same rate. Social charges can be levied based on number of employees. If there are tax advantages, they would attach to volume of sales, not business organization or formality.

2. In favour of giving special treatment to some kinds of online businesses:

Different types of e-businesses should be treated differently. They have different impacts on society that may be recognized and encouraged, or discouraged. Then how do we distinguish among them? Whether they hold a business licence, or are registered, or have a postal shipping licence? Does one form rather than another cause public policy risks – to consumers, to national trade interests, to government programs – that might suggest tighter regulation? Any of these characteristics may be a valid reason to encourage or discourage them. Use of a trading platform may or may not be a good method of distinction. The corporate form may be a good indication of the seriousness of the owners of the business. A formally structured business may have an economic impact apart from, or in addition to, sales figures, e.g. employment, related economic activity, expenditures in running the business.

Another distinction among e-commerce businesses is the role they play: do they manufacture, do they sell to wholesalers or retailers or to the public directly? Are they intermediaries in some sense? Intermediaries are required for electronic communications. What may they do or not do? The Model Laws impose few duties on communications intermediaries except for trust services. Such intermediaries are often, however, given limited immunity for what they communicate on behalf of others. (Liability issues are discussed later in this report.)

3. International perspectives

It may be of interest to consider whether and how e-commerce businesses are dealt with elsewhere, and how they are regulated.

a. E-commerce businesses

Many, probably most, countries do not distinguish the basic economic unit, e.g. a corporation, on the basis of whether it caries on e-commerce. Business registration laws tend simply to require a business of any type to register in order to carry on its activities.

For example, Estonia requires some businesses to register as businesses, not as e-commerce enterprises.[183] There are special rules for some e-commerce businesses when they register under value-added tax (VAT) regimes, but those are established at the EU level.[184]

The Central Asian republics (e.g. Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan) do not require businesses to register as e-commerce businesses. They have enabling statutes to allow enterprises to deal electronically, once they are established. [185]

The pattern in the United States is to allow e-businesses to form – incorporate, usually – under the laws of general application. They may then be subject to laws that are more focused on risks of electronic communications, like privacy or computer security rules.

A general study of regulations and policies in APEC countries in 2020 canvasses various incentives to do e-commerce but does not suggest any specific barriers to creation or general operation because of the nature of the business.[186]

Even China, which actively oversees e-commerce, suggests that entities it calls "e-commerce operators" "shall go through market entity registration according to laws,"[187] meaning the laws

[183] Incorporate, *Establishing an e-commerce business in Estonia*, undated, online: https://blog.incorporate.ee/e-commerce-business-in-estonia/#establishing_an_e-commerce_business_in_estonia. See also Republic of Estonia, Estonian Tax and Customs Board, *For Sole Proprietors*, online: https://www.emta.ee/en/business-client/registration-business/businesses/sole-proprietors

[184] Estonian Tax and Customs Board, *Special Schemes of e-commerce and services,* online*:* https://www.emta.ee/en/business-client/taxes-and-payment/value-added-tax/special-schemes-e-commerce-and-services

[185] Asian Development Bank, E-Commerce in CAREC countries: laws and policies, August 2021, online: https://www.adb.org/publications/e-commerce-carec-laws-policies. The international consultant on the present report was the lead author of that publication.

[186] APEC Electronic Commerce Steering Group, *Regulations, Policies and Initiatives on E-Commerce and Digital Economy for APEC MSMEs' Participation in the Region*, online: https://www.apec.org/docs/default-source/Publications/2020/3/Regulations-Policies-and-Initiatives-on-E-Commerce-and-Digital-Economy/220ECSGRegulations-Policies-and-Initiatives-on-ECommerce-and-Digital-Economy-for-APEC-MSMEs-Particip.pdf.

[187] E-commerce Law of the People's Republic of China, 2018, art. 10. Online: https://ipkey.eu/sites/default/files/documents/resources/PRC_E-Commerce_Law.pdf

applicable to any business (market entity). Such operators are defined to include any form of business organization.

> "e-commerce operators" mean the **natural persons, legal persons or unincorporated organizations** that engage in the operational activities of selling goods or providing service through Internet and other information network, including e-commerce platform operators, operators on platform and ecommerce operators selling goods or providing service via their self-built websites or other web service.[188] [*emphasis added*]

The same Law exempts very small businesses from registration: "cottage craft by individuals, labor services using his skills that require no license under the laws and odd and petty transaction activities of an individual, or those not subject to industrial and commercial registration."[189] However, these small operations still need to pay tax in the usual way. The general principle is at article 4 of that Law: "The State shall accord equal treatment of online and offline commercial activities and promote their integrated development."

However, other countries do focus on e-commerce businesses as such. For example, the Lao People's Democratic Republic has a Decree on the topic.[190]

> Electronic commerce has three forms as follows:
>
> Trading via Trader's electronic commerce channel [i.e. through one's own website];
>
> Trading in Electronic Marketplace [i.e. through a trading platform];
>
> Providing Trading in Electronic Marketplace [i.e. trading platforms themselves].

Each form of e-commerce business must register as such and provide prescribed information to the government in order to have permission to carry on business. The Decree describes the duties of e-commerce businesses of each class.e.g. the information to be provided on websites, and the characteristics of e-commerce contracts they enter into.[191]

---

[188] China, Law on Electronic Commerce, footnote 190, article 9.
[189] Footnote 190, article 10.
[190] Lao PDR, *Decree on E-Commerce* No. 296/GOV, 2021, articles 6 – 17.
[191] Descriptions of the law and its effects are at VDB/Loi, "L**ao PDR's new e-commerce decree – what to look out for?", October 29, 2021, online:** https://www.vdb-loi.com/laos_publication/lao-pdrs-new-e-commerce-decree-what-to-look-out-for/. **See also Tilleke & Gibbins, "Laos issues e-commerce Regulations", July 26, 2021, online:** https://www.tilleke.com/insights/laos-issues-e-commerce-regulations/.

b. Who regulates e-commerce businesses?

Just as e-commerce businesses tend to be created under general laws, so too they tend to be regulated by the same public authorities that govern offline or bricks-and-mortar activities. It is very rare for a country to have a dedicated agency just to regulate e-commerce. This statement is subject to two qualifications:

- The agency that regulates businesses generally, or businesses in a sector of the economy, may have special rules or even special laws that apply to the e-commerce operations of the entities that it regulates. They may also have special expertise in how electronic communications affect their tasks. Nevertheless, the administrative and policy benefits of a single authority prevail over any inclination to separate out supervision of just the electronic operators.

- Some areas that are well known challenges for e-commerce may be given to specialized regulators. For example, privacy rules are often the domain of expert regulators, as are consumer protection rules. However, these bodies are experts in and enforcers for offline as well as online compliance with these rules. There is not a privacy commissioner for online threats to personal information and a different one for offline threats.[192] The agency to protect consumers protects them whether they do business electronically, in person or by post. Normally the same police forces that investigate, for example, commercial fraud will investigate it whether it is cybercrime or paper crime. Again, there may be specialists within the agency for different ways of committing the crime.[193]

As a general matter, the goods and services traded in electronic commerce are the same in those in traditional commerce. The regulation of their trade can thus be entrusted to the same authorities. For apparent exceptions like digital products like texts, music or video, only the support medium is different. The principles of regulation are not different. Thus the regulator need not be different.

[192] For example, the Federal Trade Commission in the United States is responsible for fair trade practices at the national level. It has developed the concept of these practices into a broad requirement for privacy policies, both online and off.

[193] It is also possible that some challenges in computer crime raise questions of national security that would justify being remitted to a specialist agency dealing, for example, in official secrets.

c. “The State of the Art”

It is frequently estimated that certain countries are more “successful” in developing a digital economy. International ratings of digitall prosperity may rank them consistently high. Are there lessons that Mongolia can learn from them?

At this point the report will briefly review experiences of Australia, New Zealand, Thailand and Georgia.[194]

[**NOTE:** *This part will be written later. The general theme – based on a review of Australian and NZ and a quick look at Thailand – is that their plans for a digital economy depend on policies and investments and perhaps culture, but NOT laws and regulations. AU and NZ have quite hands-off e-transactions laws, with no requirements for digital signatures, for example. They tend to trust parties to figure it out. TH and GE may be more prescriptive. The authors of this report have not yet figured out why they are considered to be good examples. (NZ ranks in the top three of successful digital economies in some books.)*

In short, there is not much value to our report in looking very deeply at the law of these countries, but since they were mentioned, it may be helpful to mention them. Their lessons may be valuable, just not law-focussed.]

4. Trading Platforms

We have seen that many who engage in e-commerce use a special kind of intermediary, a trading platform, to make themselves available for trade. It probably makes sense to legislate on the relationship between trading platforms and their customers – buyers and sellers – with an eye to the public interest in the honest and effective conduct of such platforms, including fair competition and intellectual property rules. There may be taxation elements as well.

We saw earlier in the report the kinds of conditions that Shoppy.mn subjects itself to. A law could insist on that, or set limits or requirements on such conditions, to promote the protection of consumers or individual privacy. Other Mongolian platforms would be subject to the same rules.

[194] The countries were noted as successes at an ADB meeting in Manila in mid-2022 and their names mentioned in the workshop considering this report in draft form on 16 December 2022.

Applying the rules to foreign platforms might be more of a challenge, if they do not have offices or assets in Mongolia. On the other hand, if they wanted any benefits from their activities in the country, such as special tax status or rules on limitation of liability, they could be wiling to comply with local requirements to attain local advantages. There are certainly precedents for regulating foreign trading platforms. Vietnam has detailed provisions on the topic, as do Japan[195] and China,[196] and they are not alone.[197]

[195] Ministry of Economy, Trade and Industry, *Digital Platforms*, online: https://www.meti.go.jp/english/policy/mono_info_service/information_economy/digital_platforms/index.html

[196] Brookings Institute, "China's New Regulation of Platforms", Sept. 14, 2021, online: https://www.brookings.edu/blog/techtank/2021/09/14/chinas-new-regulation-of-platforms-a-message-for-american-policymakers/

[197] Baker McKenzie, "Vietnam: New Draft Law on e-Transactions Targeting Digital Platforms," 4 May 2022, online: https://www.connectontech.com/vietnam-new-draft-law-on-e-transactions-targeting-digital-platforms/

By way of example, here is a description of Vietnam's new rules, set out in Decree 85, effective 1 January 2022.[198]

3. Foreign Entities Active in E-commerce
3.1 General
Decree 85 now covers all foreign traders, organisations conducting e-commerce activities. They are classified into three groups:

- foreign traders, or organisations having e-commerce service websites in Vietnam;
- foreign traders or organisations being sellers on Vietnamese e-commerce trading platforms; and
- foreign investors in the e-commerce sector.

3.2 Specific requirements for foreign entities
Group A
Under Decree 85, foreign entities that have either:

- Vietnamese domain names (e.g. **.vn**); or
- Vietnamese as an available language; or
- More than 100,000 transactions per year are sourced from Vietnam.

shall be considered as *foreign traders, or organisations providing e-commerce service websites in Vietnam*. Accordingly, they must register for e-commerce business lines in accordance with relevant laws and either:

- set up a *representative office* in Vietnam; or
- *appoint an authorised representative* in Vietnam in accordance with Vietnamese laws.

Group B
Foreign traders and organisations that sell products on Vietnamese e-commerce trading platforms are now subject to know-your-client procedures. These are to be implemented by the local e-commerce trading platform service providers.

Group C
Decree 85 also imposes additional conditions on foreign investment into the Vietnamese e-commerce sector. In addition to complying with market access requirements under the Law on Investment 2020, foreign investors must adhere to particular market access conditions set out in Decree 85.

In 2002, Vietnam introduced much more ambitious legislation that controls trading platforms in great detail, imposing special obligations on "large platforms". (Baker McKenzie, above, footnote 192) 3

[198] ACSV Legal, Vietnam: New General And Import/Export Rules For E-Commerce Activities, 28 January 2022, online: https://www.mondaq.com/international-trade-investment/1155266/new-general-and-importexport-rules-for-e-commerce-activities

One Asian example of legislation on trading platforms is the Law on electronic commerce of the Kyrgyz Republic.[199] It defines "trading platforms" as "a set of software and hardware that ensures the sale of goods and/or works and/or services via the Internet." The trading platform provides a forum for sellers of goods to put their wares on the market, presumably in the expectation that sellers do not have the skills or equipment themselves to address the Internet directly.

The obligations of trading platform operators in the statute include making the seller's goods and services available; keeping separate the seller's and the platform operator's interests; creating a policy for users of the platform "ensuring the quality of goods and services" and "protecting the interests of consumers and information of a personal and commercial nature;" providing the ability to search the platform for goods or services sorted by price, sales and other criteria, and assisting participants in an electronic transaction in protecting their rights and interests.

The obligations under the Kyrgyz law do not distinguish between platforms run outside the country but accessible within it, and platforms operated within Kyrgyzstan.

Some countries go well beyond Kyrgyzstan in regulating trading platforms. The Vietnamese law was mentioned above. It contemplates many different kinds of platform with different rules applicable to each. It expressly applies to foreign-based platforms as well as to domestic ones.

China goes even further. Its Law on Electronic Commerce (2018)[200] has 20 articles on trading platforms, setting out rules for many possible relationships and imposing civil and administrative penalties on platform operators for non-compliance. Some critics say that the control is exercised more to collect information on platform users than to help consumers or merchants. In any event, its terms seem to focus on abuse of monopoly powers rather than simple consumer protection.[201] It too applies to platforms based outside the country, in respect to their activities in the Chinese market, as well as to domestic platforms.

[199] Law on Electronic Commerce of the Kyrgyz Republic, 2021, online: https://cis-legislation.com/document.fwx?rgn=136937
[200] China, *E-Commerce Law (2018)*, footnote 190.
[201] For a pro-China review of the platform regulations, see Wen Sheng, "China improves regulation of platform economy, not weakening it," Global Times, 8 August 2021, online: https://www.globaltimes.cn/page/202108/1230851.shtml?id=11.

It may be thought, however, that the regulation of platforms with the broadest economic and legal impact is in the recent legislation of the European Union. The Digital Markets Act[202] and the Digital Services Act[203] focus strongly on platforms. A quick summary is here:[204]

> Among the actions encompassed by the [Digital Single Market][205] strategy, the Digital Services Package, composed of the Digital Services Act (DSA) and the Digital Markets Act (DMA), is of particular interest to e-commerce. The DSA imposes new obligations on online intermediaries such as online marketplaces, social media platforms, app stores, and booking websites, while the DMA introduces new rules for large online platforms, called *gatekeepers* by the DMA. Together, these regulations aim to ensure transparency, better consumer protection, clear responsibility, liability rules, and enhanced competition between market players.

International trade bodies like the WTO, notably through its Joint Initiative on electronic commerce (which Mongolia participates in), tend to prescribe regulation with a light hand, minimalist interference with the choices of business on how they operate.[206] A growing number of laws on trading platforms are not following this prescription.

By comparison, the Kyrgyzstan model seems very modest. However, it is important to keep in mind the regulatory resources demanded by more ambitious coverage. Mongolia should review the experiences of its merchants and consumers with the platforms available to them before deciding which approach will best suit its needs. Perhaps it could let the "great powers" of e-commerce establish global standards for the global platforms, then apply the eventual consensus or model provisions in the Mongolian setting.

Regulating other areas of e-commerce

Once the basic framework for transactions is established in law, one can turn to the more specific fields of regulation mentioned. This section of the report will review the legal elements of the three

[202] EU press release on Digital Markets Act, 2022, online: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1978
[203] EU press release on Digital Services Act, 2022, online: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2545
[204] Digwatch, E-Commerce and Trade, undated, online: https://dig.watch/topics/e-commerce-and-trade
[205] EU Digital Single Market strategy, description at Wikipedia: https://en.wikipedia.org/wiki/Digital_Single_Market
[206] WTO, Joint Initiative on E-Commerce, online: https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm. Some of the draft texts in that process deal with limitations of intermediary liability; others propose more general rules on e-commerce. The "winner" of the debates remains to be decided.

main areas mentioned (consumer protection; privacy; security) and other topics and describe the best practices for a regulatory framework that Mongolia could consider in order to promote e-commerce. Mongolia has made notable progress in many fields, more could still be done in some cases, and efforts to harmonize what they have done or will do can help build regional growth through electronic means.

A final word of background: regulatory measures depend on the ability of the state to administer and enforce them.

- One may recommend consumer protection measures, but is the government capable of running a consumer services bureau and helping the people who need it? Is there a trusted court system or other dispute resolution process available to people whose new rights are not respected?
- One may recommend privacy laws requiring informed consent and high standards of secure storage of personal data, but can the state afford and find or train inspectors to check that the laws are being followed, and officials to compel compliance if the inspectors find it deficient?
- One may recommend strict measures against cybercrime – unauthorized access to computers, spreading malware – but does the state have the technical expertise to follow cybercriminals through the "darknet" and around the world to put an end to this activity?

C. Consumer protection

International best practices

A good source of inspiration for consumer protection principles are the United Nations Guidelines for Consumer Protection, most recently updated in 2015.[207]

Member states should establish consumer protection policies that encourage:

- Good business practices
- Clear and timely information for consumers to contact businesses
- Clear and timely information about goods and services sold
- Clear, concise and easy to understand – and fair – contract terms
- A transparent process for cancellation, returns and refunds
- Secure payment mechanisms
- Fair, affordable and speedy dispute resolution
- Consumer privacy and data security
- Consumer and business education

Moreover:

- Consumer protection agencies should have adequate resources

The main Mongolian *Law on consumer protection* dates from 2003, but work is at an advanced stage on a new law. The comments here focus on the draft law rather than the one still in force from twenty years ago.[208]

The new draft is a comprehensive and modern statute that sets out in detail the rights and duties of 'entrepreneurs" - sellers and manufacturers of goods and of services and those of consumers. It addresses the quality of goods (and services), threats to health and safety arising out of them, problems of delivery, timing and payment, and other issues.

The Law provides for enforcement in a number of ways, including adjustments in price and penalties for non-performance by sellers. It has a very thorough scheme for the administration of complaints at several levels, from complaints to the entrepreneur through the assistance of non-governmental organizations to the Consumer Information and Service Centre and ultimately the

[207] Online: https://unctad.org/system/files/official-document/ditccplpmisc2016d1_en.pdf.
[208] Source: Authority for Fair Competition and Consumer Protection of Mongolia

"state administrative organization responsible for the protection of consumer rights." This organization is currently the Fair Competition and Consumer Protection Agency. There is also an office of state inspector.

Enforcement of consumer rights is carried out through publicity and legal actions like arbitration and court actions, either individual or collective. Resources are available to assist consumers through several organizations, since any of these recourses may be expensive for individuals. Arbitration is more at the cost of the consumer than court actions, because the state pays the judges but the parties pay the arbitrators.

In addition, the usual criminal law prohibitions against fraud, forgery and misrepresentation apply to consumer transactions as to others.

The Law on Advertising[209] protects consumers from misleading and dishonest advertising.[210] It provides for Internet advertising, requiring – as does the draft Law on Consumer Protection – that online advertisers inform users of their name, address and a contact number.[211] Other provisions of that law are clearly intended to protect consumers in particular areas of activity or interest.

This Law prohibits or limits advertising of certain kinds of goods, such as medical supplies,[212] or advertising to certain audiences, such as children.[213]

Concerns have been expressed about the fair enforcement of these restrictions. While established businesses with a known online presence may be subject to them, will users of social media either know about the limits or be visible to the enforcement authorities? If the policies are correct, however – and they are consistent with similar rules in many countries – then the response to unfairness is to extend the reach of the Law, not cut back its scope for the advertisers with greater impact.

[209] Law on Advertising, online: https://legalinfo.mn/mn/detail?lawId=259
[210] Footnote 212, Law on Advertising article 7.
[211] Footnote 212, Law on Advertising article 12.
[212] Footnote 212, Law on Advertising, article 13.
[213] Footnote 212, Law on Advertising, article 16.

The Law on Competition[214] also protects consumers from some doubtful commercial practices like the illegal use of market dominance.[215] It also requires the Office for Fair Competition and Consumers to protect consumers in dealings in land, in meetings, and the like.[216]

Many of the obligations of sellers in the new draft Mongolian Law on consumer protection are typical consumer protection measures elsewhere, such as:

- Disclosing online of the seller's legal name and contact information and payment procedures
- "Ensuring the right of consumers to receive information about goods and services"
- Ensuring the delivery of goods or provision of services in the agreed manner and at the agreed time
- Providing contracts and history of transactions at the request of participants in an electronic transaction.

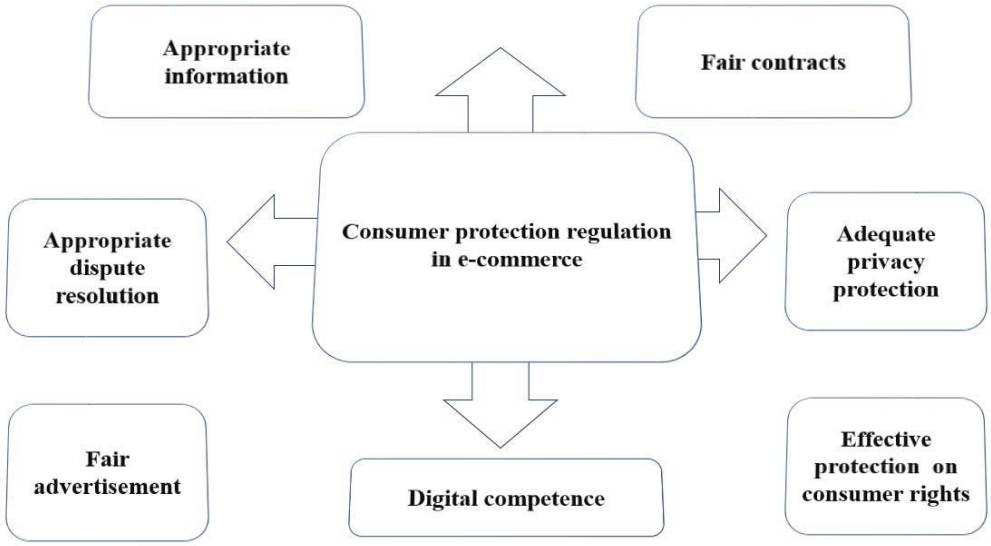
A chapter of the draft law focuses on Remote and Electronic Business Activities.[217] The main use of the "remote" provisions will be for electronic transactions. The chapter reinforces the duty to provide complete information to consumers on the location of the business and on the goods or services provided. "E-business operators" have additional obligations, as to information and as to remedies for dissatisfaction like rights to withdraw from contracts. Withdrawal rights are spelled out in detail, though subject to some limitations where withdrawal from a contract already made would not be fair to the seller.[218]If Mongolia were going to legislate on trading platforms, it is likely that the duties of a "trading platform operator" in e-commerce would include "protecting the interests of consumers."[219]

For example, the Kyrgyzstan law gives the buyer in a transaction on a trading platform the right to obtain "complete and reliable information about the good and/or services offered for purchase", and "protection of their rights in accordance with the legislation of the Kyrgyz Republic in the field of consumer protection."[220]

[214] Law on Competition, online: https://legalinfo.mn/mn/detail?lawId=12.
[215] Footnote 217 article 7.
[216] Footnote 217 articles 14 and 16 among others.
[217] Draft consumer protection law, footnote 211, chapter four, articles 17 to 21.
[218] Draft consumer protection law, footnote 211, articles 20 and21.
[219] For example, Law of the Kyrgyz Republic on electronic commerce, footnote 202, article 6 (4) e).
[220] Footnote 202, article 7(1).

There is also a suggestion that privacy matters could be addressed from the perspective of consumer protection, though the topic is treated separately in the present report.

This graphic gives a good idea of the policy situation and implications of consumer protection laws:[221]



Conclusion on consumer protection

The draft law of Mongolia on consumer protection is consistent with international best practices. It has the potential to be administered in a way that consumers are aware of their legal rights and have a practical, affordable and timely means to enforce them.

D. Privacy (personal data protection)

[221] Source of graphic: Authority for Fair Competition and Consumer Protection of Mongolia.

International best practices: Early privacy guidelines were published by the Organisation for Economic Co-operation and Development (OECD) in 1980.[222] These guidelines have been made law in whole or in part by many countries to establish the following fundamental principles:

(i) collection limitation (no more information should be collected than is needed for the purpose disclosed to the person providing the information),

(ii) data quality (the information should be as reliable as possible),

(iii) purpose specification (the data collection must disclose to the data provider the purpose of the collection and proposed use of the data),

(iv) use limitation (the data should not be used for any undisclosed purpose),

(v) security safeguards (the data should be kept and managed securely),

(vi) openness (the practices and policies of the data collectors should be knowable to those they affect),

(vii) individual participation (the people whose information is being collected and used should have the right to know what information is held and to have it corrected if appropriate), and

(viii) accountability (there should be an effective remedy for an individual for any breach of these rules by the data collector or user).

[222] OECD. 1980 (amended 2013). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. See also the convention to give stronger effect to the Guidelines: Council of Europe. 1981. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108; and Council of Europe. 2018. Modernised

The OECD revised the guidelines in 2013, while retaining many of the original principles.[223] Among the significant changes were greater emphasis on implementing and enforcing the principles and a focus on the cross-border flow of personal information that reflects the advances in global information networks and the economic value of data.

The General Data Protection Regulation (GDPR) of the European Union (EU) came into force in 2018.[224] The GDPR not only governs the internal data practices of the EU, one of the world's largest economies, but the regulation also has spillover effects by applying to the personal data that EU member states transfer to the rest of the world. Data collection by international companies in the EU is also governed by the GDPR. The basic obligations that the GDPR imposes on data controllers in the public and private sectors are largely consistent with those that the OECD originally published in 1980.

Convention for the Protection of Individuals with Regard to the Processing of Personal Data. https://www.coe.int/en/web/data-protection/convention108/modernised.

[223] OECD. 2013. *The OECD Privacy Framework*. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[224] European Parliament and Council of European Union. 2016. *General Data Protection Regulation*. https://gdpr-info.eu/ and https://eur-lex.europa.eu/legal-content/EN/ TXT/PDF/?uri=CELEX:32016R0679&from=EN. The GDPR replaced the influential EU Data Protection Directive of 1995.

Privacy is protected in Mongolia principally through the *Law on the Protection of Personal Information*.[225] This is a modern and comprehensive statute passed in 2021 and in force since May of 2022. It has the usual features of such legislation:

- Personal data is collected only with consent of the data subject, with certain standard exceptions such as public records, protection of the health of the data subject, and the like.[226] The collector of the data has detailed obligations to ensure that the consent is informed.[227]
- Some sensitive information (health, religion, sexual preference) is subject to stricter controls and fewer exceptions to consent.[228]
- Personal information stored for archival, historical, statistical purposes and the like must be depersonalized.[229]
- Collection is limited to purposes disclosed at the time of collection and shall not be kept longer than that purpose requires.[230]
- Personal data held by collectors ("data controllers") must be kept secure.[231] The law goes into considerable detail on how to do this.
- The owner of the information[232] has the right to access his or her personal data and to have it corrected, updated or removed if the evidence supports such a step.[233] The right to removal seems to apply only in cases of wrongful collection or error, and not to constitute a right to be forgotten in the European sense.[234]

Data processors (who work for data controllers) and data controllers themselves must notify the owners of personal information (the people the information is about) of any violations of this law,

[225] *Law on the Protection of Personal Information, 2021*, online: https://legalinfo.mn/mn/detail?lawId=16390288615991
[226] Footnote 228, articles 6 and 7.
[227] Footnote 228, article 18.
[228] Footnote 228, articles 9 and 10.
[229] Footnote 228, articles 6.2.5, 6.3, 11.
[230] Footnote 228, articles 8.10 (purpose), 15.1.3 (duration)
[231] Footnote 228 article 20
[232] Occasionally the law uses the term "data subject" – for example, in article 16.1.1. The term is not defined in the law. In other countries it is used to mean what Mongolia calls the owner of the information, i.e. the person whose personal information is at issue.
[233] Footnote 228, articles 16.
[234] Footnote 228, article 19

whenever discovered.[235] The owner of the information may "file a complaint with the relevant authorities in accordance with the law" because of such a violation.[236]

To enforce the *Law on personal information*, a chapter of the law called "Data Protection Authority" gives powers and responsibilities to both the National Human Rights Commission and the Ministry of Digital Development and Communications.

The National Human Rights Commission has extensive investigation and dispute resolution powers.[237] It is not completely clear if it has the power to make binding orders on persons or entities that have not complied with the law. Its powers seem mainly to be make recommendations, though the law does not say to whom – probably to mention them in its reports to the legislature for action.[238]

The Ministry of Digital Development and Communications is to "ensure the implementation of laws and regulations on the protection of personal information" and "cooperate with relevant organizations". Whether ensuring implementation includes the power to make binding orders on data processors or controllers is not clear.

Complaints about government collection of personal information are dealt with under the General Law on Administration. Other complaints go to "the competent authority" or the National Human Rights Commission.[239] Criminal and other penalties are provided for as well.[240]

Since the law has been in force only since May 2022, it is too early to know how this combination of powers will work in practice.

The text of the privacy legislation is largely satisfactory. It is foreseeable that some enterprises that may wish to rely on personal information of clients or of the public may need some educational

[235] Footnote 228, article 22.1, 22.2.
[236] Footnote 228, article 22.4. The "relevant authorities" appear to be the National Human Rights Commission – see article 24.1.4. However, the Commission's powers involve submitting "requirements and recommendations to to relevant authorities" – article 24.1.2. – and to "relevant organizations – article 24.1.3.
[237] Footnote 228, article 24.
[238] Footnote 228, article 24.1.6.
[239] Footnote 228, article 28.
[240] Footnote 228, article 30.

outreach from the government, likely one of the authorities named under the legislation, to ensure that they understand how to comply with the law with confidence.

The new legislation is intended to reassure consumers, particularly perhaps outside urban areas, who are worried about threats to their privacy, despite the predecessor law. Such concerns can deter them from engaging in online transactions.

Cross-border transfer of personal data

The law allows for cross-border transfers of personal information if there is a treaty with the destination country. The usual condition for such transfers, that the country to which the information is transferred offers equivalent protection for personal information, is not in the Mongolian law and probably should be. In the absence of a treaty, transfer may occur only with the consent of the owner of the information.[241]

An additional topic relating to cross-border transfers of personal data are rules that restrict or prohibit such transfers and require that personal information of a country's citizens (or residents) be processed only within the country. Such a rule is known as "data localization'. A number of countries have implemented such a rule, notably China and Vietnam. Others are tempted by it, because it sounds as if it gives added protection to citizens.

However, data localization tends to be disfavoured by free trade advocates, because it interferes with the efficient processing of data by multinational businesses. They would need to build a data server in each country for that country's data. This affects economies of scale.

In addition, data localization is sometimes used as a method for the state to control online activities of its residents, because all their data remain accessible to state authorities. This criticism has been made of both China and Vietnam in this context.[242]

The Mongolia-Japan Free Trade Agreement prohibits data localization, as do many free trade agreements, unless the measure is "necessary to achieve a legitimate public policy objective,

[241] Footnote 228, article 14.

[242] See J. Fox, "How are Foreign Investors Responding to Vietnam's New Data Localization Regulation" *Vietnam Briefing,* Sept 23, 2002, online: https://www.vietnam-briefing.com/news/how-are-foreign-investors-responding-to-vietnams-new-data-localization-regulation.html/

provided that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade." This would be rare though conceivable.[243]

E. Data protection (commercial and official data)

"Data protection" is a comprehensive term including data security, data availability, and access control. It extends beyond data privacy or the protection of personal information as just discussed.

> Data protection is focused on protecting assets from unauthorized use, while data privacy defines who has authorized access.
>
> Data protection is the act of safeguarding the data already obtained, no matter what it is (personally identifiable information, payment data or proprietary/commercial information).[244]

The law has a number of ways of protecting such data in any event:

- Trade secrets are protected by law. The main evidence found on this point is the exclusion of such matters from the access to information statutes discussed below.
    - The Law on Transparency of Public information, adopted in 2021 and in force in May 2022,[245] excludes some narrow kinds of commercial information from disclosure by public officials.
    - There is some reasonable expectation of protection of trade secrets. That protection is presumably enforced by some free-standing action, not just by enforcement of exceptions to disclosure legislation.
- Intellectual property law: by which use or copying of somebody else's data is prohibited. Besides the general protection of the law in this field, it is possible to put into a law on trading platforms that IP will not be violated by a trading platform and by intermediaries. It can provide a system by which IP rights holders may notify the seller, the platform operator or the intermediary of its rights and the recipient must cease the violation.

[243] Mongolia - Japan Free Trade Agreement, footnote 144, article 9.10.
[244] *Forbes* magazine, "Data Privacy vs Data Protection: Understanding the distinction in defending your data," online : https://www.forbes.com/sites/forbestechcouncil/2018/12/19/data-privacy-vs-data-protection-understanding-the-distinction-in-defending-your-data/?sh=281a6f6d50c9
[245] Law on the Transparency of Public Information, online: https://legalinfo.mn/mn/detail?lawId=16390263044601

- Cybercrime law: the *Criminal Code* of Mongolia prohibits unauthorized access to computer systems and he alteration of any data in computer systems.[246] This prohibition would extend to ransomware attacks.

Traditional laws protecting commercial and official data from interference or theft are generally media-neutral, so they would normally apply to electronic data.

There seems to be little free-standing specific protection of commercial data in Mongolia. Nothing in the privacy statute described in the last section extends beyond the personal information of individuals to cover other data.

It appears likely that Mongolia should legislate more clearly to actively protect the confidentiality of any data – commercial or personal – that is not in its usual state accessible to the public. Such legislation could be similar to the *Law on the Protection of Personal Information*, but it should prohibit the collection, use or disclosure of commercial or other confidential information except by express consent of the owners of the information (and such consent for commercial purposes may not be unusual among companies doing business together) or by overriding public purposes.

At present there is no clear international best practice on the topic that could be imitated, but data protection laws are in place elsewhere and can be used as models for Mongolia.

F. Remote Notarization

It is of the essence of e-commerce that transactions are not done in person but online, i.e. "remotely", no particular distance being required for the communications to be considered "remote". The earlier discussion in this report noted that the draft Law on consumer protection has a chapter on e-commerce under the title Remote and Electronic Business Activities.

One element of "remote" transactions is the authentication of the participants in them. Remote authentication became especially important with the Covid pandemic, where traditional in-person signing sessions were often avoided. The applicable law needs to contemplate practical challenges: how can remote transacting parties, or remote legal witnesses (and even notaries),

[246] Criminal Code, articles 26.1, .2 and .3. Cybercrime is discussed below in the next section of this report.

be sufficiently certain of the identity of the other parties? How can they be sure that what is being signed is what is supposed to be signed, or what is sent later? For notarization, how can one be sure that the person signing as notary is an actual notary?[247] In short, reliable authentication is needed for the participants in the signing action – signatory and witnesses – and for the document(s) being signed, at the time of signing and at the time of later use.

These questions have often been answered elsewhere by legal requirements that remote signing be witnessed on a live video feed, with parties properly identified by special software that can verify the validity of identification documents like passports or driver's licences. Digital signature systems can be set up to record each signature in order and prevent any alteration to the signed document once a signature is placed on it. Registers of notaries can be created for checking online in real time when verification is needed.

Moreover, the verification system already available under Mongolian law, using the digital certificate now included in national identity cards, may be adaptable to remote usage. People can already enrol themselves for digital signatures without showing up in person. Using these signatures in an especially secure way should be a relatively small step, at least conceptually, from where the country is now. (As noted earlier, there are questions of user comfort throughout the system, but they do not necessarily require law reform to resolve.)

Amendments to the Civil Code would be needed to permit this in Mongolia.

G. Cybercrime and cybersecurity

[247] The Law on Notary in Mongolia, footnote 23, expressly authorizes electronic notarization but does not apparently contemplate such an action happening except in person. However, a number of places in the world are considering remote notarization – there is an established legal framework for it in the United States, for example. The questions raised are similar to those for other remote signing systems, so they should not be excluded in principle.

International best practices

The standards are set by the Council of Europe's Budapest Cybercrime Convention (2001)[248]

- Prohibit any unauthorized access to a computer system
- Prohibit any unauthorized interception of non-public transmissions of computer data
- Prohibit the damaging, deletion, deterioration, alteration or suppression of computer data without right.
- Prohibit the intentional and unauthorized hindering of the functioning of a computer system
- Prohibit the unauthorized possession or sale of devices capable of committing the above offences or of computer passwords or access codes.
- Prohibit computer-related forgery and fraud
- Prohibit a wide range of activities related to child pornography

Another vital ingredient of public confidence in e-commerce is an expectation of honest conduct online.[249] Mongolia already has basic criminal laws in place prohibiting the usual forms of dishonesty, such as misrepresentation, fraud, forgery, and theft.

One may also look at the boundaries on economic activity provided by competition laws meant to inhibit the creation of monopolies and monopoly-like conduct through such activities as price-fixing, price discrimination, and bait-and-switch selling. Mongolia has a Law on Competition with such provisions.[250] These laws – including Mongolia's - are generally media-neutral: they apply to online and offline transactions equally. New legislation is not usually needed.[251]

[248] Council of Europe. 2001. *Convention on Cybercrime*. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185. An official explanatory note is also available online: https://rm.coe.int/16800cce5b.
[249] The general discussion here is drawn from the 2021 ADB study of the CAREC countries. Footnote 109 above.
[250] Law on Competition, online: https://legalinfo.mn/mn/detail?lawId=12
[251] Moreover, the Budapest Convention of 2001 requires that member states ensure that many traditional offenses remain offenses when committed online (see footnote 251).

Adding protections that cover online crime specifically aims to bolster the trust of consumers and business participants in e-commerce.[252]

The essential provisions of laws against cybercrime are widely agreed. The two treaties on the topic—one in place, one in draft form—have many common elements but take different approaches to administration. The Council of Europe Convention on Cybercrime (Budapest Convention of 2001) is very clear on the application of criminal law to online activity.[253] It aims to ensure that the 47 Council of Europe member states ban certain kinds of undesirable online conduct that might not be illegal under traditional law.[254]

The main online offenses that convention signatories are required to prohibit are illegal access to information systems (computers and networks), illegal interception of computer communications, interference with data or systems, and the misuse of electronic devices. The offenses expressly include the creation and spread of malware that harms the ability to use one's computer and that may steal valuable information. This includes viruses, worms, ransomware, and the like.

A draft United Nations convention on cybercrime is very similar to that of the Budapest Convention. It also protects copyright "and related rights."[255] The real difference turns on enforcement. It gives more autonomy to states in their own investigations than does the Budapest Convention and requires less disclosure to and cooperation with other countries.[256] It does, however, have many provisions on cooperation, information sharing, extradition, and related powers.

Crimes against computers are dealt with in Chapter 26 of the *Criminal Code* of Mongolia, Crimes against the Security of Electronic Information.[257]

[252] One study in Azerbaijan found that passing information security (cybercrime) legislation "was a critical driver of increasing consumer confidence." Asian Development Bank (ADB). 2016. A Snapshot of E-Commerce in Central Asia. *Asian Development Blog*. 18 January. https://blogs.adb.org/blog/snapshot-e-commerce-central-asia .
[253] Council of Europe. 2001. *Convention on Cybercrime, f*ootnote 251.
[254] For example, some legal systems do not traditionally recognize data as a form of property. Under existing laws, therefore, copying data without authority may not constitute theft, and deleting someone else's data may not constitute damage to property.
[255] Draft United Nations Convention on Cooperation in Combatting Information Crimes. Online: https://www.rusemb.org.uk/fnapr/6394
[256] A. Peters. 2019. "Russia and China are trying to set the U.N.'s Rules on Cybercrime," Foreign Policy. 16 September. Online: https://foreignpolicy.com/2019/09/16/russia-and-china-are-trying-to-set-the-u-n-s-rules-on-cybercrime/ .
[257] Criminal Code(2015) online: https://legalinfo.mn/mn/detail/11634

Article 26.1.1 prohibits illicit access to the data or system of computers. Just looking around is enough to commit the offence.

Article 26.1.2 makes it an offence to copy, change, hide or harm data or computers or to prevent their proper operation. Doing any of these actions in a way that interferes with the functioning of the computers of a "public authority" attracts a more severe punishment.

Imprisonment is provided for such offences committed by organized crime or against computers containing state secrets or "crucial information."

Creating or selling malware is an offence against article 26.2, if the malware provides illegal access, and against 26.3, if the malware steals or harms the contents or operations of other computers.

These days just about everybody understands that fighting cybercrime is exceedingly difficult. Cybercriminals take some pains to disguise their location and tend to attack indirectly. Consumer or user education is a crucial tool for resisting cybercrime. Making the target harder to attack is as important as fighting the attackers. The 2021 Cybersecurity Law provides for such cooperation in detail.[258] It considers the risk and the roles in all parts of society that could be exposed to cyber-risks, notably organizations with critical infrastructure, and sets out their responsibilities for security and for security audits.

It would appear that Mongolia's response to cybercrime is largely consistent with international standards, in the circumstances. The administration rather than the legislative text will be critical. The new Law on Cybersecurity aims at the administration, leaving the legislation on cybercrime itself to the Criminal Code. If Mongolia wishes to join the Budapest Convention, however, it will also want to ensure that the Code generally prohibits the general crimes listed in the Convention when a computer is used to carry them out. The Convention does not deal much with administrative procedure, except for duties of cooperation with other member states.

At a stakeholders' meeting in June 2022, a representative of the Cybercrime Division of the Criminal Police Department noted the recent increase in cybercrime in Mongolia and listed some of the difficulties that the police had in fighting it.

- The Criminal Code provisions on the topic do not mention e-commerce in particular.

[258] Law on Cybersecurity, December 2021, chapter 4, online: https://legalinfo.mn/mn/detail?lawId=16390365491061.

- Requesting and receiving information from abroad is complex and slow.
- Getting information on crimes committed online is difficult, notably from commercial trading platforms.
- Banks are slow to react to reports of crime, and obtaining authorization to ask the banks to help is also slow, so stolen assets can often be removed from the country before police can get to them.

The police had a number of proposals to help them fight cybercrime. Most involved better and faster access to information from all sources, so that approvals for intervention could be timely. Besides improving communications channels, these are the principal requests:

- Legal support to establish a special channel for law enforcement agencies to freely access, restrict, delete and neutralize user information from websites, social networks and platforms with servers abroad.
    - Such powers would need very careful definition and limitation. The risk of interfering with legitimate communication and transactions would be high, even if (or especially if) limited to sites with servers outside Mongolia.

- In the event that a victim of a crime makes a money transfer, the bank should take immediate measures to seize the money at his request, when the victim becomes aware of the problem.
    - Care would need to be taken that bank customers did not try to undo proper transactions simply because they had changed their mind. It might be helpful to provide in any such law that a person at whose request a blocking order was made must indemnify anyone harmed by the order, if the order turned out later to have been unjustified.

- Getting approval from the Prosecutor's office to monitor and restrict movements of money is slow. Administrative processes should be established to reduce the time it takes.
    - This constructive step would not appear to require changing the applicable law.

H. Electronic payments

All commerce requires payment, and e-commerce works best with e-payments. For B2C transactions, the world standard is e-payment through credit cards. The card issuer takes the responsibility for identifying and authenticating the card holder and ensures that the merchant is paid (within some contractual limits). (In Mongolia far more people hold debit cards than credit cards, but they may be used in domestic electronic transactions equally well.)

The terms of use are largely set by the large card organizations, notably Visa and Mastercard, subject to the national laws that apply.

The *Law on National Payment System* governs all money in the country, including electronic payment systems. The operation of the system is described by the central bank, Mongolbank.[259]

> The Law on National Payment System was approved on May 31, 2017 and became effective on January 1, 2018.[260] The law establishes the legal and organizational framework for the national payment system; governs the procedure for providing payment services and the activities of the participants of the national payment system; defines the organizational and operating requirements for payment service providers and operators; and sets procedures for exercising supervision and oversight with respect to the national payment system. This law also allows non-bank entities to participate in the national payment system.[261]

In addition, Mongolbank describes payment methods available in the country:[262]

- Cash
- Internet bank
- Payment orders and invoices
- Mobile bank
- Payment cards
- Remittances
- E-money
- Billing

[259] Mongolbank payment system: online https://www.mongolbank.mn/eng/listpaymentsystem.aspx
[260] Law on National Payment System, online: https://legalinfo.mn/mn/detail/12668
[261] A list of payment service providers published by Mongolbank is online: https://www.mongolbank.mn/eng/listpaymentsystem.aspx?id=4 It includes card issuers and acquirers and mobile banking processing services, among others.
[262] Bank of Mongolia, payment systems, online: https://www.mongolbank.mn/eng/listpaymentsystem.aspx

The issues with e-payments seem more technical than legal, at this point. To the extent that banks' own procedures impair the use of online transactions, they have the legal ability to relax their precautions.[263]

1. Foreign payments

The Bank of Mongolia interacts with foreign banks. In particular, "In order to develop the national payment system in conformity with the international standards and core principles, the Bank of Mongolia shall cooperate with other foreign countries' central banks and international organizations." However, the price of all transactions conducted in Mongolia must expressed in Mongolian currency.[264][265]

It has been noted that though credit cards can be used to make payment abroad, the fees on such transactions are heavy.

That said, there appear to be problems with inbound payments from abroad that hamper the ability of Mongolians to export by way of electronic transactions. Inbound payments are currently mainly remittances from Mongolians abroad. Paying businesses in Mongolia for goods shipped abroad is much harder.

The use of PayPal, for example, has been difficult or impossible for inbound payments for many years, PayPal itself said in 2017

> Unfortunately it is not completely up to us to offer this service, the main banks in Mongolia have rejected our proposal according to which PayPal could be used to receive money in Mongolia.
>
> However we're still negotiating with the local banks best possible terms for our customers.
>
> The main challenge we have is that ecommerce is not yet fully regulated in your country and until certain moves and law changes are made by the government, PayPal in

[263] A full list of laws, regulations and orders that govern the banking system is online: https://www.mongolbank.mn/listlawsandregulationsdb.aspx?id=5
[264] Law on Performing Payments in National Money Tokens, 2009, online: https://legalinfo.mn/mn/detail/484
[265] Bank of Mongolia Policy on Payment Systems, para. 4.2, online: https://www.mongolbank.mn/documents/regulation/paymentsystem/PolicyonPaymentSystem.pdf

> Mongolia can be used to send money and shop in foreign countries, but not to receive money for sales.[266]

PayPal does not specify how e-commerce should be further regulated, or what changes to Mongolian law would be necessary for the situation to change.

According to the draft UNCTAD report on e-commerce in Mongolia, the Bank of Mongolia currently says that "negotiations with respect to entry of Stripe and PayPal to Mongolian incoming cross-border payments market are ongoing."[267]

Resolving these problems would be a help to the efficiency of exporters.

It has also been noted that Mongolia's floating exchange rate can produce swings in the value of money that may discourage cross-border commerce. The relation of international money markets to cross-border e-commerce is however well beyond the scope of this report.

I. Dispute resolution

[266] PayPal community/managing my money/sending and receiving money/Mongolia (archive March 26, 2017, in a thread going back to 2014), online: https://www.paypal-community.com/t5/Sending-and-receiving-money/Mongolia/td-p/772965.
[267] UNCTAD draft report, above, footnote 26, 60.

International best practices

There are internationally recognized legal frameworks for mediation and arbitration, and for the enforcement of arbitral awards. Trading nations are well advised to adopt those frameworks:

- UNCITRAL has a complex array of Mediation texts, described here: https://uncitral.un.org/en/texts/mediation aimed at fair procedure, neutral mediators, and enforceability of the results of the mediation.
- The UNCITRAL Model Law on International Commercial Arbitration sets out the rules for such an arbitration and ensures that the arbitrator can function without undue supervision by national courts of either party. The opportunities for judicial intervention are limited.
- The New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards is the international standard for the enforcement of awards. It ensures that awards can be enforced in any of the 100+ member states of the Convention. Mongolia has been a party to this Convention since 1996.

Legal rights are of little use if they cannot be enforced when needed. Conflicts about the exercise of rights require some means of peaceful resolution. The traditional method of resolving such disputes is the public court system, capable of dealing with civil disputes (mainly between private parties or involving private interests) and criminal disputes (where matters of public order and safety arise.)

However, courts can be expensive, slow and hard for some people to understand. In international disputes, parties may not trust judges in the courts of the adverse party. As a result, less formal alternatives have developed. The main alternative dispute resolution methods are mediation and arbitration.

- Mediation involves a neutral person intervening between or among the disputants, ensuring the continuance of discussion, the generation of options for moving forward, and the framing of an eventual compromise if the mediation succeeds. The mediator has no power to impose a resolution.

- Arbitration also involves a neutral person hearing the disputants but relies more on resolving their legal rights. The arbitrator has the power to impose a resolution.

Both mediation and arbitration are known in Mongolia. The advantage of either process over the general courts, besides avoiding expense and exposure of the dispute to the public eye, is that the parties may arrange for an expert in the subject-matter of the dispute.

Most arbitrations in Mongolia are submitted to the Mongolian International and National Arbitration body.[268]

> [M]ediation centers operate at courts of first instance (court-based mediation centers), and may operate at government authorities, NGSs and professional associations (other mediation centers).[269]

In international disputes, mediation and arbitration have the additional advantage that the neutrality of the mediator or arbitrator can be arranged. Disputants do not have to trust the national court system of their adversaries.

It is important to the credibility of the system that settlements resulting from mediation and arbitral awards be enforced, if the parties do not comply with them automatically. The Law on Arbitration of 2017[270] provides for such enforcement. The law as a whole is clearly influenced by the UNCITRAL Model Law on International Commercial Arbitration.[271] It also provides for enforcement by a court if required, and for awards made outside Mongolia, according to the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards[272], to which – as noted earlier – Mongolia is a party.

In passing, it is noted that the UN Model Law on International Commercial Arbitration now allows the use of electronic documents for arbitration agreements and arbitral awards. Mongolia's Law on

[268] KhanLex Partners, Dispute Resolution, online: https://khanlex.mn/expertise/dispute-resolution/
[269] LehmanLaw Mongolia LLP, Alternative Dispute Resolution: Finalizing Mediation, online: https://lehmanlaw.mn/blog/alternative-dispute-resolution-finalizing-mediation/
[270] Law on Arbitration (updated, 2017), online: https://legalinfo.mn/mn/detail?lawId=12456
[271] UNCITRAL Model Law on International Commercial Arbitration, online: https://uncitral.un.org/en/texts/arbitration/modellaw/commercial_arbitration
[272] Convention on the Recognition and Enforcement of Foreign Arbitral Awards, online: https://uncitral.un.org/en/texts/arbitration/conventions/foreign_arbitral_awards

Arbitration[273] follows that lead. Article 8.3 says that an arbitration agreement shall be in writing, but this is qualified by several subsequent provisions:

> 8.5. The requirements set forth in Paragraph 8.3 of this law shall be deemed to have been met in the form of information exchange, if it is possible to access and use the information contained in electronic communication.
>
> 8.6. 'Electronic communication' shall mean any communication that the parties make by means of data messages.
>
> 8.7. 'Data massage' shall mean information generated, sent, received or stored by electronic, magnetic, optical or similar means, including electronic data interchange, electronic mail, and telegram, telex.

Returning to the topic of mediation,

> Settlement agreements executed by mediators of a court-based mediation center become a sort of court judgment, as judge of corresponding court issues a court decision confirming such settlement agreement. And if parties fail to voluntarily perform their obligation under settlement agreement, it shall be enforced same as court decision. On the other hand, while settlement agreements executed by mediators of other mediation center[s[are also binding for parties of dispute, these are not enforced [in the same way] as settlement agreements executed by [a] mediator of [a] court-based mediation center. If parties fail to voluntarily perform the obligations under such settlement agreement, parties have the right to pursue their claims in other forums (such as litigation or arbitration.)[274]

[273] Law on Arbitration, footnote 273.
[274] LehmanLaw, footnote 272. See the Law on Conciliation, online: https://legalinfo.mn/mn/detail/8689?fbclid=IwAR1lSAhAsGf9TPFyJRUtYymD40EXNaMgAOXMszAmdekmM7BmJeze-NPsCR4. Articles 7 and 8 distinguish between court-connected and other mediators, and article 27distinguishes the enforcement of agreements concluded with the support of each kind.

There are also international instruments for the enforcement of agreements to settle international mediations.[275] It appears advisable for Mongolia to accede to and implement the UNCITRAL Model Law on International Commercial Mediation and International Settlement Agreements Resulting from Mediation, 2018.[276] Recourse to mediation is much more attractive if it does not have the prospect of litigation at the end of it, to enforce a settlement that when it is made appears voluntary.

The modern version of alternative dispute resolution is online dispute resolution (ODR). Sometimes ODR just means a regular mediation or arbitration conducted by videoconference over the Internet. More often, however, it can rely on software that leads parties – normally to a mediation – through structured questions and responses, helping to narrow the differences between them – and sometimes ending with an agreement. Designing such systems can be difficult and require expertise in the subject-matter of the dispute. It can also be difficult to get both sides to potential disputes to agree to participate before any dispute has arisen between them. In some national legal systems, such an agreement (before a dispute arises) would be unenforceable. It may be that operating rules for trading platforms could overcome this disparity in policy.

There is no current plan to introduce ODR to Mongolia.

J. Civil liability: private enforcement of good conduct

The law of civil liability helps to compensate people harmed by the faults of others.[277] At the same time it may dissuade people—including businesses and manufacturers—from committing those faults in the first place. States designing the civil law framework of domestic and cross-border paperless trade must therefore examine who will participate in this trade, the relationships between the trading partners (buyers and sellers), what can go wrong, and who should bear the risk of this happening (i.e., who is best positioned to avoid the potential harm or best able to take out insurance against it).

[275] Office of Democratic Institutions and Human Rights, *Opinion on the Law of Mediation of Mongolia*, online: https://www.osce.org/files/f/documents/c/5/458395.pdf para 98.
[276] The Model Law is online: https://uncitral.un.org/en/texts/mediation/modellaw/commercial_conciliation
[277] This discussion is substantially drawn from the ADB report on e-commerce legislation in CAREC countries, footnote 130.

This calculation is made more complicated as many participants in a cross-border electronic trade system are public institutions—either government entities, such as customs services, or bodies performing public functions, such as inspection laboratories like GASI in Mongolia.

The participants in electronic commerce transactions depend on numerous intermediaries to manage and carry their communications: internet service providers, e-commerce trading platform operators, and trust service providers. For cross-border trade, there are also regulatory authorities, notably the Customs Authority, and possibly a National Single Window to coordinate approvals for their goods and services to cross the border.[278]

However, other policies may complicate the imposition of liability, for example the desire to ensure that the intermediaries continue in business, rather than being crippled by large judgments, and the public agency character of the intermediary (like a single window or the regulatory agencies). Many countries limit the exposure of taxpayer-funded bodies to substantial money judgments.

To date there is little experience in Mongolia with civil liability imposed on the intermediaries of e-commerce, either domestic or international. The Communications Regulatory Commission has advice for customers of Internet and other communications service providers, though at the final level it refers them to the competition authorities.[279] The essential consideration for present purposes is the liability of intermediaries. For this purpose, “intermediaries” include providers of logistics, communications (notably web hosting, data storage and cloud computing) and financial services to the primary participants in e-commerce, being the seller, buyer and platform operator.

Ideally a law touching this topic would provide that an intermediary is not liable for the legality of transmitted or stored electronic messages or goods and services, so long as the intermediary is not the originator of transfer or placement of communications and does not change the content of electronic messages and documents when providing communications services.

Such provisions seem satisfactory in principle. There are no suggestions in the literature on behalf of traders or others that they are problematic. They are very much in the mainstream of intermediary liability rules around the world. For example, the Global Network Initiative, a multistakeholder body with an interest in technology, opposes imposing liability on

[278] As noted earlier, the Mongolian Single Window is a long-term project but inevitable with time.
[279] Communications Regulatory Commission, Frequently Asked Questions, online: https://www.crc.gov.mn/list/customer/mn?show=134

communications intermediaries for what they carry for others.[280] One may consider as well the Manila Principles on Intermediary Liability,[281]a product of national and international media and digital rights bodies (so not yet "international best practices" in the same sense as in other parts of this report.).

It is also desirable that any special limitations of liability should be disclosed at the outset of a transaction or of a commercial relationship, before trading begins, so that potential traders (inside or outside the country) can evaluate their risks. Trading websites or government-sponsored facilities like single window operations are well suited for this kind of disclosure. Sometimes the limitations can be imposed by contract.

However, where the participants can be considered private commercial operations, perhaps subject to competition, then the normal rules of civil liability can be more easily allowed to function.

Civil liability is helpful to bring discipline to a trading system only if recourse to the civil courts is accessible for the parties to disputes. Alternatives to court processes have already been discussed and may also be acceptable forums to determine liability.

[280] Global Network Initiative (GNI), *Intermediary Liability and Content Regulation,* undated, online: *https://globalnetworkinitiative.org/policy-issues/intermediary-liability-content-regulation/*
[281] *Manila Principles on Intermediary Liability,* 2015, online: https://manilaprinciples.org/principles.html

VI. RECOMMENDATIONS FOR DEVELOPMENT OF THE LAW

Responding to challenges – overview of policy dynamics[282]

When weighing the roles of the private sector and state legislative and legal regimes in expanding e-commerce and their contribution to an economy, two issues stand out. The first is the ability of the private sector to conduct e-commerce without further reform. The second is the desirable degree of autonomy for the parties to e-commerce. Both involve assessments of risk and reward and the consideration of two basic questions:

(i) **Is law reform necessary?** In many parts of the world, e-commerce grew before laws were changed. This growth was based on contracts between businesses (trading partner agreements) and on the flexibility of existing laws that allowed novelty. However, there were and are limits to how far private agreements could go to changing basic rules of law. Law reform was more economical of effort and more general of application than contractual regimes. Central Asian countries like Mongolia tended to leave little room for private initiative until the basic laws were enacted to allow for electronic documents and signatures. This study discusses further reforms that go beyond what transacting parties can do for themselves. This section starts with the current law in place and considers building on it.

(ii) **How much regulation or party autonomy should there be?** The degree of regulation required by or wanted in a system greatly depends on the extent of risk the system is willing to tolerate. These risks fall into three broad categories:

a. ***Risk to the transacting parties themselves.*** Are the parties able and competent to make good decisions in novel areas? They may be free to fail, or the state may feel obliged to save them from bad choices. If the latter is the case, then the state is more likely to regulate the choices that lead to the risks. The state may

[282] This text is largely influenced by sections of the ADB E-Com publication *E-Commerce in CAREC Countries: Laws and Policies*, Footnote 130.

distinguish among parties to "save", protecting consumers more than businesses, for example.

b. ***Risk to others.*** A less regulated system may expose others potentially affected by business-to-business (B2B) or business-to-consumer (B2C) dealings to fraud or mistakes. Some societies are more willing than others to trust the competence and honesty of private actors; others rely on more extensive state oversight of economic activity.

c. ***Risk to public policy.*** Governments differ in how much uncertainty they can tolerate, and in deciding how much business failure should be allowed, and at what cost to the economy. Innovation has benefits and costs.

Risk tolerance differs between parties and states. It is a policy question, not a technical one, and law reform is a form of risk management that reflects this level of tolerance. In part to minimize the need for state regulation, Mongolia may want to support the development of private sector capacities to manage risk.

A. The statutory framework

Mongolia currently has a collection of statutes affecting electronic commerce (though no law directly about electronic commerce), electronic signatures, though no law directly about electronic governance, access to public information, consumer protection (soon to be updated), the protection of privacy, and cybercrime, to name only the main ones. While they all deal with elements of electronic commerce, it would make little sense to consolidate them, roll them up into one comprehensive statute on electronic communications.

A good argument can be made that the various statutes do largely have their own distinguishable topics. It may be easier to find the answers to one's questions in separate statutes than in one very large piece of 'omnibus' legislation. The more important question to ask is consistency: do these laws contradict each other or do they work together well?

In practice, efforts have been made to keep the statutes consistent. When one is amended, others that relate to it have tended to be amended at the same time. Four separate but related statutes were all amended at the same time in late 2021, for example, and came into force together in 2022.

It is important when such statutes are being amended that input is sought from all sectors of the economy likely to be affected. Some kind of legislative working group is indicated, with public and private sector participants. All relevant ministries need to be involved, though sorting out their respective responsibilities can be a challenge. Interest groups should be invited to be at the table. In many cases, financial institutions would need to be part of the discussion, especially since the e-payments system is in need of facilitation.

IT IS RECOMMENDED that the diverse e-commerce statutes now in place should not be consolidated, but that law reform efforts focus on keeping them all co-ordinated when any of them are being amended. A working group on any such amendment should include those principally affected by the proposed amendment, in the public as in the private sector.

Reform initiatives should be undertaken for these items:

1. Electronic transactions, e-commerce and trading platforms

A law governing electronic commerce should be enacted to govern several aspects of the use of electronic communications for commercial reasons. Besides typical transactions, already well covered by the Civil Code, the new laws should provide for the phenomena of e-commerce beyond strict transactions, such as the topics dealt with in the UNCITRAL Model Laws on Electronic Commerce and, as necessary, on Electronic Signatures. A likely model for such a law could be the UN E-Communications Convention, adapted for domestic application.[283] It should also set out basic rules for electronic trading platforms and ensure that agreements to buy and sell on such platforms are legally valid and subject to appropriate controls. Those provisions can be related to the proposed Law on consumer protection and the new Law on privacy where appropriate, along with fair competition principles. Restrictions on the ability of people and

[283] Its adaptation for this purpose is discussed in the Appendix to this report.

businesses to agree to transact electronically, including through trading platforms, should be kept to the minimum required to achieve important public policy objectives.

2. Electronic signatures

The Law on electronic signatures should be clarified as to when it is acceptable for transacting parties to use e-signatures that do not qualify as digital signatures. What strength of authentication do they need? What other legal assurances can they offer? The UNCITRAL principles of technology neutrality should apply in at least some circumstances.

The authentication mechanisms of the e-Mongolia initiatives on electronic government seem appropriate at present. Future questions in those initiatives should so far as possible be resolved consistently with the principles in this report.

3. Protection of personal information

The law about transferring personal information of Mongolian citizens and residents outside Mongolia should ensure that the place where it is transferred offers equal legal protection to the information – whether this is a matter of treaty or domestic law in that place. The consent of the owner of the personal information to such a transfer should be informed by knowledge of this equivalence or lack of it.

On the other hand, it is problematic to require personal (or commercial) data relating to Mongolian residents to be processed and stored only in Mongolia. This "data localization" policy creates inefficiencies for cross-border enterprises, requiring them in effect to build separate data processing facilities in each country with such rules. Any such policy should be strictly limited, as in the Mongolia-Japan Free Trade Agreement.[284]

4. Data protection

Mongolia should legislate more clearly to actively protect the confidentiality of any data – commercial or personal – that is not in its usual state accessible to the public. This could build on the current protection for trade secrets and related commercial information, the source of which

[284] Footnote 144. See discussion, section V.D, text at footnote 228.

is harder to locate than it should be. Such legislation could be similar to the *Law on Personal Information.* It should prohibit the collection, use or disclosure of commercial or other confidential information except by express consent of the owners.

5. Cybercrime and cybersecurity

The ability of law enforcement authorities to expeditiously restrain the transfer of funds in cases of apparent or alleged fraud should be clarified, but subject to strict limits on the duration of the restraint and probably to the need for the person alleging fraud to indemnify any person improperly harmed by the restriction on the transfer. Consultation with financial institutions would be required to design an effective mechanism with appropriate safeguards for all interests.

6. Civil Liability

The liability of communications intermediaries for harm done by what is communicated should be clarified in law, notably with respect to user-generated content, along with the intermediaries' right to limit their liability by contract with their clients. The Manila Principles on the liability of intermediaries should be a guide to such a law.

B. Longer term government plans

The government of Mongolia has recently ended its Smart Government plan and begun its Digital Nation plan, running to 2027. This was discussed in section I.3 above. At present it is not clear that the plans will require legislative support, as distinct from the increasing use of technology. The elements of the Digital Nation plan are: Digital infrastructure, e-Governance, Cybersecurity, Digital Literacy, Innovation and Production, and National Development Accelerator. Only e-government and cybersecurity need laws and regulations in support, and those elements have been discussed above. If artificial intelligence plays a role in the program, then it may call for regulation as well. Regulation in that field has challenges keeping up with the capacity of the technology. Other elements, such as infrastructure and digital literacy, may benefit from governmental support, but it is not clear at this stage whether that would involve legislation.

C. International issues

A constant theme of any writing on law and e-commerce is the desirability of harmonizing one's laws with that of one's neighbours and trading partners. Electronic trade flows naturally across borders with electrical and communications systems, and the more the law on both sides of the border is compatible, the easier it is for traders to participate. This report has mentioned a number of possible international instruments in which Mongolia could be engaged.

As noted earlier, Mongolia is already a party to many of the principal relevant international instruments, notably

a. ESCAP Framework Agreement on Facilitation of Cross-Border Paperless Trade in Asia and the Pacific. The Framework Agreement promotes a high common standard for paperless trade law and also offers facilities for exchange of expertise and some financial assistance in complying with its term.

b. WTO Trade Facilitation Agreement – Mongolia should continue implementing the TFA in a diligent and orderly manner.

c. UN Convention on the Use of Electronic Communications in International Contracts. The ECC helps standardize the law initially developed for the UNCITRAL Model Laws, for international contracts. It also gives the opportunity to interpret other treaties consistently with them where they affect contracts. The ECC can and probably should be used as the basis for a domestic law on electronic transactions, as discussed earlier.

IT IS RECOMMENDED that Mongolia accede to or adopt the following instruments, in descending order of their desirability or importance.

1. UNE/CEFACT Recommendations for the National Single Window

   When legislating to create the National Single Window, close attention should be paid to the CEFACT standards, which have created expectations among international traders. The standards should be statutory and not merely based on a series

of interlocking contracts among the principal market participants.

2. UNCITRAL Model Law on Electronic Transferable Records

   As traders become ready to accept electronic versions of bills of lading, warehouse receipts and the like, Mongolian law should recognize the standards of reliability set out in this Model Law.[285] This Model Law is being adopted relatively slowly around the world. Advice may be taken from the principal trading partners as to timing.

3. International Standards Organization

   Expert advice should be sought on how and when to impose the ISO's Series 27000 standards on technological operations in Mongolia. They are the international state of the art.

4. Regional Comprehensive Economic Partnership (RCEP)

   Consider whether Mongolia's trading partners are joining RCEP; if so, accede as well to maintain the advantages of free trade. The e-commerce provisions of RCEP are largely compatible with current Mongolian law and with the standards of the ESCAP Framework Agreement mentioned earlier.

5. UNCITRAL Model Law on Identity Management and Trust Services (2022)

   Verify that Mongolian law is consistent with it in its treatment of trust services, so far as appropriate for dealings with its principal trading partners.

[285] Footnote 163.

CONCLUSIONS

Mongolia has done some constructive and imaginative law reform on electronic commerce over the past years. Its current collection of statutes holds up well on analysis for domestic purposes and also in comparison to its major trading partners.

Many countries have similar agendas in these pandemic or post-pandemic times, to support online trade and the ability of their residents and businesses – and regulators – to participate in it.

Thus harmonization is a top priority. It is important to build linkages both formal and informal to bodies with a harmonizing agenda.

This report has examined Mongolian law in the light of international standards and has considered the opportunities to advance harmonization. Its marks are quite good, though a few steps remain to be taken, notably to support e-documents and e-signatures more broadly. Where paperless trade – domestic and cross-border – is not happening, the cause is often not deficiencies in legislation or regulation but in technology and culture, and in financial resources to take advantage of the opportunities that do exist.

Our competence and our mandate have, however, been limited to legislation and regulation. In our view, following the recommendations in the last section of the report will help Mongolia advance its digital economy agenda in step with its neighbours and trading partners. We hope that the results will justify our optimism.

THE END

APPENDIX

[from *Regulatory framework for e-commerce development in the CAREC*]

Using the Electronic Communications Convention as domestic law

John D. Gregory

22 March 2020

Convention on the Use of Electronic Communications in International Contracts

The Electronic Communications Convention is intended to increase the degree of harmonization of national and international legal regimes enabling electronic commerce, by laying down a standard universally acceptable text that would bind all parties and not, like a model law, be subject to local variance around the world.

The Convention builds on the Model Law on Electronic Commerce (and not really on the Model Law on Electronic Signatures, though it is consistent with that model law too.) It resembles the model laws in being a facilitative rather than a regulatory instrument.

There are differences between the Model Law on Electronic Commerce and the Convention. Some of them have been mentioned in the part above on enacting the Model Law; they are largely improvements or refinements of the analysis in the intervening years, and a state interested in enacting the Model Law, or just bringing it up to date, would benefit from following the Convention's wording on point.

Other differences arise from the different purposes of the two instruments.

- The Convention applies only to contracts, not to other areas of law, as the Model Law does.

- The Convention excludes contracts for personal, family or household purposes, notably (though not only) consumer contracts.[286]
- The Convention excludes certain regulated financial transactions, normally governed by their own system rules.

States interested in the Convention need to decide whether they wish its regime to apply to domestic as well as to international matters. Some states have done that. If they have already enacted the Model Law (the usual case to date[287]), they will need to amend it to conform with the Convention. If they have not yet enacted the Model Law, they will need to enact some of its provisions to make up for places where the Convention does not apply.

Several states have implemented the Convention without acceding to it, just to use it as a general-purpose electronic commerce statute. To the extent that their law would be the applicable law in an international matter, they get the benefit of the Convention either because of their consistent domestic law or because the Convention's terms would make the Convention apply to the transaction according to the law of the other state affected, if it were a member state of the Convention.

The following analysis reviews the situation where the state contemplating the Convention already has the Model Law in place. Much of the analysis would apply if the state were also contemplating enacting the Model Law.

WHY ADOPT?

The main reason to adopt the Convention is to help build consistent rules around the world for using e-communications in international contracts. (Countries that signed the Convention while it was open for signature may ratify it; others may accede. The legal effect is the same; thus the use of "adopt" to cover both processes.) For the internal purposes of a state with the Model Law on Electronic Commerce, it does not need the Convention's rules; its own laws allow for e-communications in negotiating, making and performing contracts. Likewise, the laws of many of its major trading partners will probably accommodate e-communications, though not always on identical terms.

[286] Electronic Communications Convention, EXPLANATORY NOTE BY THE UNCITRAL SECRETARIAT, online http://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf para 74
[287] For example, Singapore and Sri Lanka. Australia began this process but has not yet completed it in all states.

However, many countries do not specify that e-communications can be used with legal effect in their systems, and those that do so specify may do so in different language or use different concepts. It is not always possible in negotiating a contract to agree that one's own domestic law will apply. It would therefore be an advantage to have an accepted international standard on the point.

It may make sense for countries that are already familiar with e-commerce laws, and especially those whose e-commerce laws are inspired by the Model Law on Electronic Commerce, to become a party to the Convention. By doing so they declare to the international community that they consider the Convention's rules to be acceptable, based on their experience.

The Convention's rules apply to the medium for making international contracts. It is a separate question, discussed below, whether its rules should be adopted domestically at the same time. Those who think that its rules are not ideal, or even undesirable, may wish to oppose their adoption at home. However, this view need not stand in the way of accession for international uses. As noted, there is no guarantee that the law applicable to an international contract will be one's own domestic law, and the Convention may well be preferable either to uncertainty about the use of the electronic medium or to the application of even less desirable rules found in the domestic law of the other party.

WHEN THE CONVENTION APPLIES

On its face, the Convention applies to communications about contracts when the parties are in different countries. What makes the Convention apply to those circumstances? The law applicable to those communications may be the Convention because it is the law of both parties' countries, or because it is the law of one of the parties' countries and that law applies to the contract by choice or operation of law.

Article 19(1) allows any Contracting States to declare that it will apply the Convention only when the states of both parties are Contracting States, or when the parties have agreed that the Convention will apply.

Article 3 allows parties to opt out of the Convention, so if they do not want it to apply, they can avoid it. Similar rules apply to the application of the United Nations Sales Convention. States party to that Convention may decide if they have experienced problems with its application. The

ability of parties to transactions to limit the application of the Convention may make states less likely to opt out or limit its scope for all purposes.

The Convention facilitates using technology to create contracts. It may be thought that international commerce would benefit from a broad application, rather than finding ways to restrict it.

APPLICATION TO OTHER CONVENTIONS

The Convention applies to communications about international contracts where those contracts – including communications with respect to them - are subject to the general law of contracts of one of the parties' states. It also extends its rules to communications about international contracts governed by other conventions. Article 20 spells out six United Nations Convention that fall into that category: the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards,[288] the United Nations Sales Convention,[289] and conventions on limitations periods,[290] the liability of operators of transport terminals,[291] independent guarantees and stand-by letters of credit[292], and the assignment of receivables.[293]

Applying the E-Communications Convention to these conventions does not amount to amending them; amending them would be a cumbersome process. It merely says that the use of electronic communications in association with contracts that they govern will be understood as in the E-Communications Convention. This is a very useful means of encouraging the legally effective use of e-communications. UNCITRAL believes that there is little if any risk in allowing for e-communications under these conventions, for a country that was prepared to accept the Convention itself.

The Convention goes further to apply similarly to international contracts governed by any other international convention to which a Contracting State to the Convention is now or later becomes

[288] Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York, 10 June 1958)
[289] United Nation Convention on Contracts for the International Sale of Goods (Vienna, 11 April 1980)
[290] Convention on the Limitation Period in the International Sale of Goods (New York, 14 June 1974) and Protocol thereto (Vienna, 11 April 1980)
[291] United Nations Convention on the Liability of Operators of Transport Terminals in International Trade (Vienna, 19 April 1991)
[292] United Nations Convention on Independent Guarantees and Stand-by Letters of Credit (New York, 11 December 1995)
[293] United Nations Convention on the Assignment of Receivables in International Trade (New York, 12 December 2001)

a party – whether or not it is a United Nations treaty and whether or not that treaty existed at the time this Convention came into force. (Article 20(2)).

However, Contracting States are allowed to tailor this application with respect of other conventions by a series of opting out and opting in decisions. The result is that Contracting States may have a general rule accepting the Convention's rules for other conventions except as specified, or a general rule rejecting the Convention's rules for other conventions except as specified. The 'other specifications' can exclude any of the six listed conventions as well as others not named. In short, a Contracting State may apply the Convention to whatever other conventions it chooses, but the default is that it applies to electronic communications respecting the formation and performance of contracts under all such conventions.

Would a state need to review the terms of every convention to which it is a party, to see if any rules applicable to international contracts that might be affected by the Convention are consistent with those of the Convention? Or should it take a chance on acceding without declaring any exclusions? The Convention allows a Contracting State to make a declaration or a revised declaration at any time, so if a problem is discovered in the future, the acceding state could exempt contracts governed by the problematic convention at that time.

The government of Singapore in 2009 concluded on this point that there was no reason to prevent the Convention from applying to all conventions to which Singapore was a party, for three reasons.[294]

(a) The domestic e-commerce statutes already applied to contracts under those additional conventions, to the extent that the contracts were governed by Singapore law.

(b) Matters in which the use of electronic communications may be a cause for concern are excluded from the domestic law and can be excluded from the Convention through the use of article 19(2). See the discussion below.

(c) The extension of the Convention to other conventions has a narrow effect. It merely achieves functional equivalence for electronic communications in connection with the formation or

294 Singapore (Info-communications Development Authority and Attorney General's Chambers), *Joint IDA-AGC Review of* Electronic Transactions Act *Proposed Amendments 2009*, (Report), LRRD No.1/2009, para. 2.10.6, available at http://app.agc2.agc.gov.sg/DATA/0/Docs/PublicationFiles/ETAReport_LRRD1of2009.pdf.

performance of a contract to which the other conventions apply. It does not affect the substantive legal questions governed by those conventions.

It appears likely that having the Electronic Communications Convention applying to the interpretation of a contract subject to another convention in the acceding state would be good news to a party to such a contract, if the party has chosen to communicate electronically in respect of that contract. A default choice to have the Convention apply to contracts under all other conventions seems like a low-risk option.

INTERNATIONAL AND DOMESTIC APPLICATION

UNCITRAL's mandate is international trade law, so the Convention is drafted to apply to international contracts. However, it is also drafted to work as a domestic law on contractual communications where the Contracting State has no existing law on that topic.

What should happen when a Contracting State already has good law on that topic, notably the Model Law on Electronic Commerce? Should it have a 'dual system', one law for communications about international contracts and one about communications for domestic contracts? Or should it bring its domestic law into conformity with the international rules so it can apply the same law to all?

It will be noted that some of the terminology of the Convention is a bit different from that in the Model Law. Acceding to a convention means applying its terms as written; a Contracting State may not change them. If the state objects to any of the rules or wording of the Convention, then perhaps it should not try to implement them for its domestic law as well.

<u>In favour of having a single law</u> (i.e. amending the domestic law to conform with the Convention)

- The Convention is almost the same in substance as the Model Law on Electronic Commerce, so its provisions are largely acceptable and tested in practice in the acceding state.
- To the extent that the Convention's rules are new, they are better than those in the Model Law.
- Parties should not be caught by surprise by having different rules depending on where the other party is. This is particularly important for electronic transactions, which may attract foreign parties (although the Convention applies only if the parties know or ought to know

that they are in different countries – Article 1(2)).

- It may be thought that harmonization between the Convention and domestic legislation is desirable to avoid the possibility of two different sets of rules for similar transactions. The impact of these differences will not likely be significant. However, it is always possible that judicial examination of these differences could result in unanticipated interpretations.

In favour of having a dual regime (i.e. the Convention for international contracts and the Model Law for domestic ones)

- There may be established interests in the domestic regime, businesses that have set up their practices in accordance with it, who do not want any change.
- Since the legal effect of the Convention is almost the same as that of the Model Law, parties will not be prejudiced if they find themselves bound by the unexpected rules of the international regime of the Convention (assuming one has added the Convention – international - to the Model Law – domestic).
- Parties may opt out of all or any part of the Convention, including by conduct (such as a draft of a contract) that is inconsistent with it. They are not trapped in any event, so long as they can agree on an alternative. It should be noted in this connection that the Convention itself is rarely mandatory: it says how e-communications are to be treated if the parties choose to use them. It does not require anyone to use or accept information in electronic form, though some of its rules are mandatory once e-communications are chosen.

In practice, some states that have become parties to the Convention have harmonized their domestic law to it, and some have not. A few have implemented the Model Law at the same time as the Convention.

EXCLUSIONS AND PERMISSIONS

A. Harmonizing exclusions from the Convention and from domestic law

The Convention excludes from its scope consumer contracts (contracts for personal, family or household purposes), transactions “on a regulated exchange” (essentially sophisticated financial transactions among institutions that already have their legal rights in electronic communications

spelled out satisfactorily among themselves), and bills of exchange, promissory notes, and other transferable documents of title.

The Model Law allows states to exclude an indefinite list of transactions or documents. Each country thinking of acceding to the Convention should compare its list with those of the Convention. It may be that some exclusions are appropriate domestically and not internationally. Others may appear useful at both levels.

Through the use of article 19(2) of the Convention, a member state can exclude from its application any of its domestic exceptions, either because it believes that the exceptions are right in principle for international as well as for domestic transactions, or just to keep the domestic and international laws consistent.

Those provisions of its domestic law that the enacting state does not exclude from the Convention should be adapted to operate consistently with the Convention. That may be done globally by a provision in the legislation to implement the Convention to the effect that the legislation prevails over any contrary rules in matters governed by the Convention.

B. Harmonizing permissions in domestic law and the Convention

It may be harder to decide what to do when the domestic law is more open to e-communications than the Convention. There are several examples:

- The Model Law applies to consumer contracts (though it yields to specific consumer protection rules), while the Convention excludes such contracts.
- The domestic rule on the validity of electronic signatures may be broader than either the Convention or the Model Law.
- The time of sending an electronic message is measured in the Model Law from the time the message arrives in a system outside the control of the sender, while the Convention now measures it from the time the message leaves a system within the control of the sender. This may be a distinction without a difference. The reason that the Model Law chose the time of entry into another system is that system logs were thought to record the time of entry of messages but not the time of departure. The difference is a question of evidentiary focus and

not of any significant difference in the actual time.[295] On the other hand, it may come down to an allocation of risk: who has to prove, and who is better able to prove, when the message either left one system or entered another?

- The time of receiving an electronic message is measured in the Model Law from the time the message has entered an information system designated or used by the addressee and is capable of being retrieved. The Convention speaks of the message being capable of being retrieved at the electronic address designated by the addressee. It is unlikely that the different wording will produce different results on this point.

Is a Contracting State allowed to permit the use of e-communications more broadly in international contracts than the Convention provides? The parties to such contracts can expand on the Convention, though not so as to undermine protections for integrity of the communications. So parties could not rely on the Convention – as implemented in the state whose law made it applicable – to validate an e-signature but by agreement purport to extend the validation to an e-signature that did not meet the tests of article 9 of the Convention. However, the Convention takes such agreements into consideration in applying its tests of reliability of the signing method.[296]

It is arguable that parties to international contracts would want to rely on the limits to the Convention, and not just to its permissions, so finding themselves subject to e-signatures that do not meet the Convention's standards, or finding their contracts voidable for unilateral error more broadly than the Convention requires, may be unwelcome to them. However, parties are free to opt out of the Convention in whole or in part, so could “reinstate” the original Convention limits if that is what they preferred.

Although Contracting States may not change the provisions or the scope of the Convention, to what extent must the Convention displace the otherwise applicable domestic law? Where the Convention sets out rules, those rules prevail, as in the e-signature example above. But where

295 The Australian Information Industry Association wondered how one would apply a test depending on the sender's control of the system, when the sender may be using 'software as a service' or cloud computing, and not technically ever have control of the system it uses – since it is by definition someone else's system. Letter from the Association to Helen Daniels (January 28, 2009) available at: http://www.ag.gov.au/Documents/Submission%20from%20the%20Australian%20Information%20Industry%20Association.PDF. It may be thought that systems subject to 'control' would be read to include systems that are obliged by contract to follow the sender's instructions.

296 ECC Explanatory Note, footnote 19, paragraphs 14, 85, 86 and 137.

the Convention does not apply at all, then the applicable domestic law can supplement it. This is routine analysis for matters such as civil liability or the substantial validity of contracts: the Convention leaves such issues to the domestic law.

The Convention does not apply to consumer transactions. Will the applicable domestic law on such transactions apply to international contracts? The parties to those contracts should not be surprised to find international consumer contracts covered by somebody's domestic law. The Convention's exclusion of consumer transactions should be treated only as a limit inherent in UNCITRAL's mandate, not affecting the desirability of some rules to be applied to the transactions. If the general law of a contracting state on electronic communications applies to those communications, then the parties will be able to rely on that law – including the consumer protection measures that are also part of the applicable law.

This is consistent with the approach of the Model Law on Electronic Commerce, which applies to consumer contracts but which yields to otherwise applicable consumer protection law.

Moreover, it should not be forgotten in this discussion that the Convention applies only to communications related to contracts, while the Model Law applies to all uses of electronic communications not expressly excluded. So long as domestic law reflects the Convention with respect to the contracts that it covers, nothing in the Convention limits the application of the domestic law to non-contractual communications or communications about other contracts, domestic or international.