

The views expressed in this presentation are the views of the author and do not necessarily reflect the views or policies of the Asian Development Bank Institute (ADBI), the Asian Development Bank (ADB), its Board of Directors, or the governments they represent. ADBI does not guarantee the accuracy of the data included in this paper and accepts no responsibility for any consequences of their use. Terminology used may not necessarily be consistent with ADB official terms.



ADB/CAREC Presentation E-Commerce Legislation

John D. Gregory
Legal Consultant
Toronto Canada

CAREC Institute Virtual Workshop
28 May 2020

Overview

- Nature of electronic communications
- Global solutions
 - Removing the barriers: UNCITRAL
 - Regulating the rest
- Role of private sector in e-commerce: does it need law reform?
- International commercial and trade initiatives
- Agendas for CAREC member states
- Appendix: CAREC members' laws & recommendations

Electronic communications in general

- What is the problem with electronic communications?
 - Results are subject to manipulation and deterioration
 - Everything is done by combinations of 1s and 0s
 - Altered states may be hard to distinguish from originals
 - Information requires computing device to display – risk of error
- Traditional laws use words that do not readily apply to information in digital form, e.g. writing, signature, original
 - These laws are barriers to use of e-communications

Law reform – phase 1

- Removing the barriers – United Nations Commission on International Trade Law (UNCITRAL)
 - **Model Law on Electronic Commerce** – MLEC (1996)
 - **Model Law on Electronic Signatures** – MLES (2001)
 - UN Convention on the use of Electronic Communications in International Contracts (**Electronic Communications Convention**, or ECC) (2005)
 - Model Law on Transferable Electronic Records - MLETR (2017)
- Nearly 80 countries have implemented all or part of the MLEC
- Fewer have implemented all or part of the MLES
- Some CAREC members have implemented some parts of MLEC
- One CAREC member has adopted the ECC (AZE)

UNCITRAL principles

- The UNCITRAL texts are all built on the same principles:
 - **Functional equivalence:** electronic information is not the same as information on paper but should be legally effective if it can perform the same policy function as its paper equivalent.
 - **Technology neutrality:** the law should not specify what technology e-communications must use to serve as functionally equivalent to paper-based information.
 - **Media neutrality/non-discrimination:** the law should give equal effect to information on paper and in electronic form.
 - Information shall not be denied legal effect solely because it is in electronic form.
 - **Minimalism:** law reform deals only with the impact of new media and does not otherwise affect substantive legal rules.

Law Reform phase 2

- More than minimal change is desirable.
- **Privacy** – the key principle is informed consent of the individual
 - The global standard is Organization on Economic Cooperation and Development (OECD) Guidelines and Council of Europe Convention to implement the Guidelines
 - Leading example: EU General Data Protection Regulation (GDPR)
- **Cybercrime** – the key principles ban unauthorized access to data and harming data (malware)
 - The global standard is the Council of Europe (Budapest) Convention
 - But Russia has proposed an alternative treaty to the UN, supported by China
- **Consumer protection** – the key principles are timely information about e-transactions and the ability to remedy error or wrongdoing.
 - The global standard is UN Guidelines for online consumer protection

A CAREC Agenda - Background

- **Legislation and regulations are only one element of electronic commerce:**
 - Economic development: computers, infrastructure, innovation & rewards
 - Cultural views: risk tolerance, doing business with strangers, comfort with immaterial things
- **Self-regulation vs state regulation**
 - Initiative vs need to control
 - Competence to choose vs hand-holding
 - Private interests vs public policy
- **State capacity to regulate**
 - Accrediting and disciplining certification service providers
 - Overseeing best privacy practices, enforcement
 - Investigating and prosecuting cyber-crime
 - Offering consumer protection directly, creating liability regime, dispute resolution

Role of Private Sector

- Two elements of the role of the private sector
 - Ability to function without reform
 - Degree of party autonomy
- 1. **Do we need law reform?**
 - In North America, much e-commerce was done before laws were changed
 - Based on contracts ("trading partner agreements")
 - Based on flexibility of common law that allowed novelty
 - General principle: commercial law reform should follow commercial practice, not try to lead it
 - BUT need to fill gaps, protect parties or non-parties from new risks
 - Piecemeal reform is inefficient, causes uncertainty, expense
 - Let the lawyers stop worrying and give firm opinions

More on private sector role, impact

- 2. **Party autonomy**: how much regulation should there be?
 - Risk to the parties themselves – ability to make good decisions in novel areas – competence? freedom to fail?
 - e.g. authentication, e-signatures
 - Risk to others – exposing others (B2B, B2C) to fraud or mistake – competence and honesty
 - Risk to public policy – how much uncertainty can government tolerate? How much business failure should be allowed? Cost to the economy? To the state?

Note on risk: Different parties and different states will have different tolerance for risk. Risk tolerance is a policy question, not a technical one. **Law reform is risk management.**

Note on ADB: Can it support private sector capacity, to economize on need for state regulation?

- Q: can **private technology** offer methods of doing e-commerce securely?
 - Should law leave room for uses of devices, codes, platforms?

Electronic payments

- **B2B** – general role for the National Bank in almost all CAREC states
- Other banks take orders from National Bank, correspond with it.
 - Some Customs Authorities allow brokers or importers to establish electronic accounts from which payments (to Customs or other agencies) may be made by electronic direction.
- **B2C** – role of credit cards growing
 - International card payments widely acceptable
 - Credit cards are primary method of authenticating purchasers to merchants
 - Probably easiest to make arrangements with major international card companies
- Other financial technologies
 - Early days – AliPay, ApplePay, other non-bank service providers
 - Legal authority may be contract among users or directive from National Bank

Law reform: the key issues

- **Electronic transactions**
- Do e-documents need to be validated by e-signatures?
- Do all e-signatures need to be “secure”, generated by cryptography and supported by certificate?
 - And state role in certificate issue and management?
- Best practice: maximize room for private choice for transactions.
- **Privacy:** maintain the best, bring others up to standard
 - Need to decide how much state enforcement is possible
- **Cybercrime:** Most CAREC states seem to have the essential provisions
 - Enforcement? International cooperation
- **Consumer protection:** Helpful if legislation builds consumer trust
 - Enforcement can include international cooperation

Recommendations: domestic

Reform needed	Countries	Discussion
Adopt UN ECC for domestic law	All	Models of domestic ECC laws in Singapore, Australia, Canada (Uniform Act)
Maximize and harmonize ability to use simple e-signatures	All	Some have some flexibility but none enough.
Harmonize certification process for digital signatures	All	Is one country's model working best? State supervision needed but not necessarily state monopoly.
Harmonize cybercrime legislation with international standards	All	CAREC members are largely consistent on this point. Consider the states' capacity to enforce.

Recommendations: domestic (2)

Reform needed	Countries	Discussion
Enact modern privacy legislation	PAK, TKM	Consider the states' capacity to enforce.
Enact modern consumer protection legislation	GEO, KAZ, KGZ, MON, PAK, TAJ, TKM	Consider the states' capacity to enforce.
Establish framework for electronic payments.	PAK, UZB	All members have something in place, with exception of PAK and UZB .

International Instruments

Law reform may have recourse to international texts of different kinds,

- as inspiration for domestic legislation
- to govern cross-border trade.

- **Agreements to facilitate e-communications**
 - ESCAP Framework Agreement on Facilitation of Cross-border Paperless Trade (no standard to meet to join; can come in at any level)
 - World Trade Organization Trade Facilitation Agreement

- **Agreements on substantial law that expressly or impliedly allows e-comms**
 - Convention on the International Sale of Goods (CISG)
 - CMR Convention (on the contract for the international carriage of goods by road), similar convention on rail transport

International Instruments (2)

- **Instruments of general application**
 - UNCITRAL texts
 - UN Centre for Trade Facilitation (CEFACT) guidelines
 - International Standards Organization (ISO) standards
- **Regional trade agreements** (European Union, Eurasian Economic Union)
- Bilateral or multilateral **special purpose agreements**

Instrument	Type/scope	CAREC members as parties
UNCITRAL Electronic Communications Convention (ECC)	Global	AZE (Recommend: ALL for domestic & international)
ESCAP Framework Agreement on ... Cross-border Paperless Trade (FAPT)	Regional	AZE, CHN (Recommend: ALL)
Convention on the International Sale of Goods (CISG)	Global	AZE, CHN, GEO, KGZ, MON, UZB (Recommend: ALL)
World Trade Organization Trade Facilitation Agreement (WTO TFA)	Global	AFN, CHN, GEO, KAZ, KGZ, MON, PAK, TAJ
Revised Kyoto Customs Convention	Global	AZE, CHN, KAZ, MON (UZB upcoming)
Council of Europe (Budapest) Cybercrime Convention	Global	AZE, GEO
TIR Trucking Convention (has an electronic supplement)	Global	AFN, AZE, CHN, GEO, KAZ, KGZ, MON, PAK, TAJ, TKM, UZB
[many others for specific areas of trade]	Global/ regional	Some mentioned in the body of the report (to be published in Q3 2020). Some may authorize e-documents even if general law does not.

General law reform advice

- Facilitating law reform – advice for all countries:
 - Dedicated multi-ministry task force with support at the highest levels
 - Some variant of this group should have private-sector representation
 - Need for coordination of legal advice across government
 - All parts of government and other players need the right and capacity to communicate electronically
 - Replicate national work on international plane, and coordinate the two levels.
 - Work closely with ESCAP technical and legal working groups, if not already doing so.

Appendix

CAREC member states: situation and recommendations

Afghanistan

- Infrastructure and interpersonal trust are severe challenges.
- Afghanistan has no e-transactions legislation, though a draft was circulated in 2015.
- It has recent cybercrime and consumer protection legislation.
 - The texts are good
 - Can they be put into practice in that country?
- **Recommendations:**
 - See UNCTAD rapid e-assessment
 - ESCAP Framework Agreement (principles + team-building and resources)
 - E-transactions: UN/ECC with more weight on certificates by trusted third parties (Are there credible candidates? Can systems be purchased from abroad?)

Azerbaijan

- Azerbaijan is the only CAREC country that is a member of the E-Communications Convention.
 - The ECC requires some flexibility in authenticating electronic signatures.
- Also only one of two CAREC countries that are parties to the ESCAP Framework Agreement
 - The FA also promotes flexibility, technology neutrality
- Non-certified e-signatures are limited in use to (private) corporate information systems.
- Certification service providers are liable for some misuse of certificates.
- The law provides for some use of foreign certificates and some AZE certification of foreign service providers.

Azerbaijan (2)

- ▶ Electronic payments have a sound basis in a 2016 presidential decree.
- ▶ Privacy laws appear to meet international standards.
 - ▶ AZE is party to the 1981 Council of Europe Privacy Convention (not the 2018 update)
- ▶ AZE is party to the Council of Europe (Budapest) Cybercrime Convention.
- ▶ Consumer protection laws focus on disclosure of information. They are as good as any in CAREC.
- ▶ **Recommendations:**
- ▶ Expand scope for uncertified e-signatures
- ▶ (longer term) Join WTO, WTO/TFA

PRC

- The People's Republic of China (RPC) is the other CAREC member that has ratified the ESCAP Framework Agreement, and has to some extent brought its domestic law into accord (or it was there before..)
- China has a comprehensive e-transactions regime set out in an e-signature and an e-commerce statute.
 - Some non-certified signatures are allowed, though it is hard to know their scope.
 - A detailed regime is set out for certificates, including liability of certification service providers.
- Foreign signatures and certificates can be recognized based on administrative action acknowledging reciprocity or on international agreement.
 - It is not clear if any such action or agreement exists at present.
- The law authorizes e-payments internally and for international trade, with some duties to be performed by "platform operators".

PRC (2)

- Privacy is protected by a partial statutory regime that seems to be in development.
 - The regime has many standard elements, spread across several statutes, e.g. consent to collection, a right to have incorrect personal information deleted, etc
 - Transfer of personal data abroad or accessing it from abroad are very restricted.
 - It is not clear that any of these rules apply to government.
- The Criminal Code contains most of the usual provisions against cybercrime.
- Consumer protection rules appear to meet international standards, spread between a Consumer Protection Law and the Electronic Commerce Law.
- **Recommendations:**
 - Clarify and maximize the availability of uncertificated e-signatures
 - Complete legal privacy regime. (How is it enforced?)

Georgia

- E-transactions in Georgia are governed by a hybrid statute: some non-certificated signatures are allowed.
 - Public officials must use certificated signatures..
- Foreign e-signatures are recognized if there is an agreement with their country of origin or if the foreign standards are formally recognized by Georgia, or if a Georgia CSP guarantees them.
- Electronic payments operate in an open and modern way.
- Privacy laws are in the international tradition, though there is a long list of exceptions to the consent principle.
 - There is a personal data protection inspector to see to enforcing the rules.
- Georgia is a member of the Budapest Cybercrime Convention.
- There are no express consumer protection laws.
- **Recommendations:**
 - Become a member of the UN/ECC and UN/ESCAP Framework Agreement
 - Clarify and maximize the use of uncertificated e-signatures
 - Enact consumer protection statute on UN/OECD model + enforcement

Kazakhstan

- Kazakhstan has a technology-specific law that requires a certificated signature for an e-signature or an e-document to be legally valid.
 - The duties of the parties to a certificate signature are standard for this type of rule.
 - Rules for the management of e-documents are in part drawn from the UN MLEC.
- Foreign e-signatures can be recognized by international agreement or if approved by KAZ's "trusted third party". No criteria are set out for such recognition.
- Electronic payments are governed by a 2016 statute and regulations of the National Bank.
- KAZ's privacy law is standard for its kind.
 - KAZ has said it will administer its law in the spirit of the EU's General Data Protection Regulation (GDPR).
- The Criminal Code's cybercrime provisions are standard within CAREC.
- There is no consumer protection legislation under that name.
- **Recommendations:**
 - Become a member of the UN/ECC and UN/ESCAP Framework Agreement and CISG
 - Clarify and maximize the use of uncertificated e-signatures
 - Enact consumer protection statute on UN/OECD model + enforcement
 - develop EAEU trust framework

Kyrgyz Republic

- The Kyrgyz Republic has a very flexible hybrid e-signature system, allowing for simple e-signatures with consent of transacting parties, as well as unqualified and qualified e-signatures.
 - Unqualified e-signatures have characteristics like a reliable e-signature under MLES.
 - Qualified e-signatures have a certificate from an accredited certification service provider.
- KGZ recognizes foreign e-signatures “of the same sort” as their own, which suggests similar standards of reliability.
- Electronic payments are widely allowed under regulations by the Board of the National Bank.
- Privacy is protected by comprehensive legislation that accords with international standards.
 - Databases of personal information, called ‘arrays’, must be registered with the state.
 - Such databases must be kept secure, according to detailed provisions to this effect.
 - Cross-border transfer of personal information is done by consent or under treaty.

Kyrgyz Republic (2)

- Cybercrime provisions reflect the standard provisions among CAREC members.
- There is no consumer protection legislation under that name.
- **Recommendations:**
- Become a member of the UN/ECC and UN/ESCAP Framework Agreement and CISG
- Clarify and maximize the use of uncertificated e-signatures
- Enact consumer protection statute on UN/OECD model + enforcement
- develop EAEU trust framework

Mongolia

- Mongolia's Civil Code allows documents to be in electronic form, but they seem to need to be signed.
- The Electronic Signature Law of 2011 authorize simple electronic and certificated digital signatures.
 - It is not clear if the private parties allowed to use e-signatures actually do so.
 - State bodies must use digital signatures with certificates.
- Foreign e-signatures can be recognized if authorized by relevant foreign legislation complying with international standards.
 - State bodies are authorized to cooperate with foreign counterparts to recognize e-signatures.
- The legal system authorizes wide use of electronic payments, though not all agencies or businesses may be set up to use them yet.
- Mongolia's privacy statute dates from 1995 and is not consistent with current thinking in the area.

Mongolia (2)

- Mongolia's Criminal Code has cybercrime provisions much like those in most CAREC countries.
- Mongolia's Consumer Protection Law also dates from before e-commerce, though some of its provisions about access to information are media-neutral.
- **Recommendations:**
- Become a member of the UN/ECC and UN/ESCAP Framework Agreement and CISG
- Clarify and maximize the use of uncertificated e-signatures
- Enact consumer protection statute on UN/OECD model + enforcement
- Enact a modern privacy statute

Pakistan

- Pakistan has an Electronic Transactions Ordinance from 2002 that implements much of the UNCITRAL MLEC.
 - It also provides for advanced e-signatures created under rules as in the MLES or by an accredited certification service provider.
 - Detailed rules set out the duties of a CSP.
 - Public bodies may specify further rules for dealing with them electronically.
- Considerable progress has been made in recent years in setting up the legal and operational structures for electronic payments in the country, both for high-value business-to-business matters and more retail-focussed transactions
- Pakistan does not have a free-standing privacy statute, but some protections are scattered among other legislation, notably the statute below on electronic crimes.
- The Protection of Electronic Crimes Act of 2016 has most of the usual provisions on this topic.
 - It also contains anti-terrorism provisions and gives the state investigatory powers.

Pakistan (2)

- Consumer protection is dealt with by state not national law, and most of it pre-dates e-commerce.
 - Consumers lack awareness of the rights they do have.
- **Recommendations:**
- Become a member of the UN/ECC and UN/ESCAP Framework Agreement and CISG
- Clarify and maximize the use of uncertificated e-signatures
- Enact consumer protection statute on UN/OECD model + enforcement
- Enact modern privacy statute

Tajikistan

- Tajikistan's law on electronic documents seems to allow them without a signature or other technical standards, though it must "contain the details allowing to identify it."
- E-signatures are largely digital signatures with certificates. Rules are set out about how certificates are issued and governed.
 - There are special rules for e-signatures within a corporate information system.
 - Tajikistan reported to the ADB and the CAREC Institute that e-signatures are not used in that country.
- Electronic payments are carried out under the supervision of the National Bank of Tajikistan
- Tajikistan adopted a Law about personal data protection in 2018.
 - While its organization varies to some extent from other privacy laws in CAREC states, its content does not show significant differences.
 - The government has considerable flexibility in deciding what personal information can be transferred abroad.

Tajikistan (2)

- Tajikistan has a longer list of computer-related prohibitions than any other of its CAREC neighbours.
- There is no consumer protection legislation under that name.
- **Recommendations**
- Become a member of the UN/ECC and UN/ESCAP Framework Agreement and CISG
- Clarify and maximize the use of uncertificated e-signatures
- Enact consumer protection statute on UN/OECD model + enforcement
- Enact a modern privacy statute

Turkmenistan

- Turkmenistan's statute requires e-documents to be certified with an electronic digital signature.
 - The e-document must be displayed in a form understandable to human perception.
 - It may be used in any field of activity that uses electronic equipment.
 - The law contains rules about the operation of certification service providers ("authorized legal entities").
 - The sender and recipient of an e-document may agree on how to "regulate" the procedure for using an electronic digital signature.
- The law allows "authentication codes" in the place of electronic digital signatures but does not define what such a code is.
- There is little or no information about mutual recognition of cross-border electronic transactions.
 - The law does authorize international cooperation by use of e-documents and e-information systems and networks in accordance with Turkmenistan laws and treaties.
- E-payments are regulated by the National Bank but appear to need electronic digital signatures.

Turkmenistan (2)

- There is no specific law protecting privacy.
- Computer crime law is largely consistent with that in other CAREC countries.
- There is no specific consumer protection legislation.
- **Recommendations**
- Become a member of the UN/ECC and UN/ESCAP Framework Agreement and CISG
- Clarify and maximize the use of uncertificated e-signatures
- Enact consumer protection statute on UN/OECD model + enforcement
- Enact a modern privacy law based on international principles

Uzbekistan

- Uzbekistan law is quite complicated, with several statutes competing with Presidential Decrees and Regulations by the Cabinet of Ministers over the years.
 - The result is difficulty in knowing what e-documents and signatures are effective for what purposes.
- Most e-documents require electronic digital signatures certified by a “centre of registration”.
 - However, some documents may be supported by an “electronic message” that does not require the same formalities in order to identify its originator.
- Other laws often require e-communications to be authorized by electronic digital signature, including communications by public bodies participating in the national register of electronic state services.
- The Electronic Signature Law says that “the use of certificates of keys of electronic digital signatures of foreign states is performed according to the procedure established by the legislation.” It is not clear what legislation is referred to.
- Electronic payments are accepted in Uzbekistan but payment documents need an electronic digital signature.
- Further reform is included in the current five-year plan for e-commerce legislation

Uzbekistan (2)

- A 2019 statute sets out privacy rules much like those in other CAREC countries.
 - A new provision limits the use of automated data processing (i.e. artificial intelligence) as the basis for decisions about people's rights, except on consent.
 - The statute appears to apply to the government's own collection and use of personal information.
- Uzbekistan has a single but comprehensive article in the Criminal Code serving the usual ends of cybercrime laws.
- There is no consumer protection law as such, but e-commerce sellers must "observe requirements of the legislation on the competition and about consumer protection in case of sales of goods (works, services) in electronic commerce."
- **Recommendations:**
 - Become a member of the UN/ECC and UN/ESCAP Framework Agreement
 - Clarify and maximize the use of uncertificated e-signatures
 - Enact consumer protection statute on UN/OECD model + enforcement
 - Develop closer links with EAEU
 - Consolidate laws at different levels, clarify what is in force.



Questions?

john@euclid.ca