Legal and Regulatory Challenges to Facilitating E-Commerce in the ASEAN

[working draft only]

Dr Eliza Mik
Singapore Management University

1. Introduction

E-commerce is commonly portrayed as a contributor to economic growth and an integrating force for the ASEAN. The facilitation of e-commerce is largely associated, if not synonymous, with the harmonization of the relevant laws and regulations in this area.[1] Unsurprisingly, ASEAN is the first developing region to prepare a unified e-commerce legal framework.[2] To date, harmonization efforts have centered on electronic transactions laws, the assumption being that the latter will facilitate e-commerce by creating legal certainty for the recognition of electronic contracts. [3] The creation and harmonization of broader e-commerce laws and regulations may, however, be insufficient. As e-commerce often involves high volume and low value cross-border transactions, its facilitation may require more prosaic endeavors, such as coordinating customs procedures, tax rates and invoicing standards.[4] Moreover, the provision of a *legal* framework for e-commerce will not guarantee its success or promote its adoption. The viability of e-commerce depends on the existence of a robust telecommunication infrastructure, user-friendly online payment systems and efficient distribution networks, particularly with regards to last mile-delivery.[5] The creation of a conducive legal framework for cross-border e-commerce must therefore be regarded as part of a larger picture, comprising multiple regional initiatives addressing a wide spectrum of issues. This chapter is confined to a discussion of the challenges inherent in the regulatory and legislative initiatives aiming at promoting of e-commerce in the ASEAN.

[1] See generally: e-ASEAN Framework Agreement (2000), Article 5; ASEAN Economic Community Blueprint 2025 (2015); ASEAN ICT Masterplan 2015.
[2] Reference Framework for Electronic Commerce Legal Infrastructure (2001) ("Reference Framework).
[3] See: United Nations Conference Trade And Development, 'Review of E-commerce Legislation Harmonization in the Association of Southeast Asian Nations' (2013) ("UNCTAD Review") for a state of adoption of electronic transactions laws, p. 8.
[4] The ASEAN Single Window initiative aims to expedite cargo clearance and promote regional integration by enabling the electronic exchange of border documents, see: http://asw.asean.org.
[5] See generally: AT Kearney, 'Lifting the Barriers to E-Commerce in ASEAN' (2015) CIMB ASEAN Research Institute; UNCTAD, 'Maximizing the Development Gains from E-commerce and the Digital Economy' (2017) TD/B/EDE/1/2.

Electronic copy available at: https://ssrn.com/abstract=3100578

1.1 Scope of Discussion: The Blueprints

To delineate the scope of the discussion, it is worthwhile comparing the ASEAN Economic Community Blueprint 2015 ("Blueprint 2015"), adopted in 2008, with the ASEAN Economic Community Blueprint 2025, adopted in 2015 ("Blueprint 2025"). The Blueprint 2015 aimed at implementing the ASEAN Economic Community (AEC) by 2015.[6] It declared the need to establish the "legal infrastructure for electronic commerce and enable on-line trade in goods (e-commerce) within ASEAN through the implementation of the e-ASEAN Framework Agreement and based on common reference frameworks."[7] The planned actions included:

(1) the preparation of domestic legislation on e-commerce,

(2) the development, implementation and harmonization of the legal infrastructure for electronic contracting and dispute resolution, and

(3) the mutual recognition of digital signatures.[8]

The Blueprint 2015 also mentioned the need to develop consumer protection measures, including the establishment of the ASEAN Coordinating Committee on Consumer Protection (ACCCP).[9] It envisaged that between 2008-2009, Member Countries would enact their e-commerce laws, implement harmonized principles for electronic contracting and online dispute resolution services, adopt a regional framework for the mutual recognition of digital signatures.[10] Between 2010-2011, Member Countries were to update and/or amend relevant legislation in line with regional best practices in e-commerce, adopt guidelines on other cyber-law issues (i.e. data privacy, consumer protection, etc.) and advance cross-border electronic transactions through the mutual recognition of foreign digital signatures.[11] Between 2014-2015 a harmonized legal infrastructure for e-commerce was to be in place. In sum, the Blueprint 2015 focused on the transactional aspects of e-commerce and on the mutual recognition of digital signatures. Consumer and privacy protections were addressed only marginally. According to the 2013 UNCTAD report, the aims of the Blueprint 2015 have been largely achieved, especially concerning the enactment of legal instruments focused on electronic contracting.[12] The current Blueprint 2025 emphasizes financial integration and the development of

[6] ASEAN Economic Community Blueprint 2015, p 2.
[7] ASEAN Economic Community Blueprint 2015, p 23, para 59.
[8] ASEAN Economic Community Blueprint 2015, p 23, para 59.
[9] ASEAN Economic Community Blueprint 2015, p 19, para 42.
[10] ASEAN Economic Community Blueprint 2015, Strategic Schedule, p 53.
[11] ASEAN Economic Community Blueprint 2015, Strategic Schedule, p 53.
[12] UNCTAD Review, p. 5.

Electronic copy available at: https://ssrn.com/abstract=3100578

retail payment systems to bolster cross-border online transactions.[13] More importantly, it acknowledges that e-commerce requires innovative ways of protecting and *promoting* the interests of consumers. This in turn requires comprehensive national and regional consumer protection systems enforced through effective legislation, redress mechanisms and public awareness.[14] Unsurprisingly, the establishment of an ASEAN consumer protection framework is regarded as a key strategic measure – particularly in e-commerce.[15] In addition, the Blueprint 2025 emphasizes the need to develop inter-operable, mutually recognized, secure, reliable and user friendly e-identification and authorization (electronic signature) schemes.[16] In comparison to its predecessor, the Blueprint 2025 adopts a more practical and consumer-centered approach, recognizing that the promotion of e-commerce necessitates more than a broad declaration that contracts can be formed electronically.

1.2 Roadmap & Caveats

Throughout the discussion, it must be remembered that ASEAN does not have the advantage of a legal superstructure permitting a EU-style top-down approach to create a unified regime that could support regional e-commerce. Consequently, the facilitation of e-commerce largely depends on the adoption of common reference frameworks that can serve as legal "templates" guiding the enactment of domestic laws and regulations in the respective ASEAN jurisdictions. The choice of an adequate reference framework, accompanied by its consistent implementation and enforcement, is therefore crucial. With this in mind, this chapter critically reviews existing initiatives aimed at facilitating e-commerce, with particular focus on the selection of appropriate models to guide regulatory and legislative efforts. Given their centrality, it commences with a clarification of the term "e-commerce" and "e-commerce laws." Following the recommendations made in the Blueprints, it examines (1) the promotion of the UNCITRAL Model Law on Electronic Commerce ("MLEC")[17] as a template guiding the enactment of e-commerce legislation; (2) the claim that e-commerce requires the use of electronic and/or digital signatures – a claim that logically precedes issues surrounding the mutual recognition of such signatures; (3) the challenges of creating harmonized and innovative privacy and consumer protection regimes. The chapter addresses regulatory and legislative initiatives concerning substantive law, not mechanisms of implementation or enforcement. Before proceeding, it is pertinent to differentiate between:

[13] ASEAN Economic Community Blueprint 2025, p 7-8.
[14] ASEAN Economic Community Blueprint 2025, p 10-11.
[15] ASEAN Economic Community Blueprint 2025, p 24.
[16] ASEAN Economic Community Blueprint 2025, p 24.
[17] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment (1996) with additional article 5 *bis* as adopted in 1998.

(a) commercial dealings and dealings with public authorities, i.e. between e-commerce and an area popularly referred to as e-Government. While many legislative and regulatory initiatives include provisions that facilitate both types of interactions, this chapter addresses only *commercial* interactions enabled by the Internet. Many provisions in e-commerce instruments, such as the production of originals, the retention of records or the creation of electronic identities may, of course, be relevant for both areas.

(b) e-commerce and ICT infrastructure, i.e. between commercial interactions *enabled by* the Internet and the underlying infrastructure *comprising* the Internet. The latter is a precondition of e-commerce but is usually regulated in different legal areas, such as telecommunications law. It is crucial to emphasize that laws and regulations addressing the investment in and promotion of ICT infrastructure do not, theoretically, fall in the category of e-commerce.

1.3 Defining "e-commerce"

The OECD defines "*e*-commerce" as "the sale or purchase of goods or services, conducted over computer networks by methods specifically designed for the purpose of receiving or placing orders. The goods and services are ordered by those methods, but the payment and ultimate delivery of the goods or services do not have to be conducted online."[18] Similarly, as indicated above, the Blueprint 2015 regards e-commerce as the "online trade in goods."[19] These definitions emphasize the *transactional* aspects of e-commerce and bring it squarely within the scope of contract law, a system of rules governing commercial exchanges that underpins virtually every modern market economy. The logical conclusion is that most *legal* questions in e-commerce are questions of contract law or, to phrase it differently, that the legal area most relevant to e-commerce is contract law.[20] It must be observed that the principles of contract law are formulated in broad terms and are, in most circumstances, sufficiently flexible to accommodate transactions made by modern means of communication. It is thus questionable whether discrete laws facilitating "e-commerce" are indispensable – at least with regards to its transactional aspects. Arguably, initiatives aimed at facilitating e-commerce should inquire whether contract law (or: the *contract laws* in the respective ASEAN jurisdictions) requires any amendment to enable online transaction. Three points arise:

(a) Two discrete regimes?

[18] OECD Guide to Measuring the Information Society 2011 (OECD Publishing).
[19] ASEAN Economic Community Blueprint 2015, p 23, para 59.
[20] A. Murray, *Information Technology Law* (Oxford: Oxford University Press, 2010), p. 413.

The creation of a bespoke legal regime for e-commerce accompanied by a broad definition of the term may render it difficult to ensure a *separate* co-existence of traditional and e-commerce-specific rules. The dangers of a broad definition are illustrated by the Lao Law on Electronic Transactions, which describes e-commerce as "the purchase, sale and other exchange of goods or services between individuals, legal entities or organizations *using electronic means*."[21] [my emphasis] This leaves open to interpretation whether a transaction concluded over the phone constitutes e-commerce. While phones can be regarded as "electronic means," it can hardly be assumed that the regulatory intent underlying the said provision is to introduce special rules governing transactions concluded over the phone. Should there be different rules depending on whether an order is placed on a website, at the counter or on the phone? It could be claimed that e-commerce is "just commerce" and such divisions are unwarranted. After all, the law did not change when commercial parties started using telexes or faxes. Seemingly, all regulatory initiatives should be (or should *have been*) preceded by (a) a precise delineation of the regulatory target (*what is e-commerce? what are "electronic means"*), (b) an examination whether existing rules require supplementation, and (c) a debate whether the presence of two potentially overlapping regimes is conducive to legal certainty.

(b) The neglected areas

While it is easy to proclaim the primacy of agreement in business-to-business ("B2B") transactions, the same cannot be said about business-to-consumer (B2C") transactions, particularly in the online context. Unsurprisingly, recent ASEAN initiatives focusing on promoting e-commerce emphasize the need for adequate privacy and consumer protection regimes.[22] It is crucial to point out that every ASEAN jurisdiction has laws governing commercial exchanges (i.e. contracts) but only few ASEAN jurisdictions have comprehensive laws in the areas of privacy and consumer protection.[23] It is therefore not immediately apparent why, to date, ASEAN initiatives focused on the *transactional* aspects of e-commerce, prioritizing the creation of legal instruments in an area that already has sufficient laws and is, historically, resistant to harmonization[24] – that of contract law. Meanwhile, areas with insufficient or no laws - those of consumer protection and privacy – have been neglected.

(c) The "law" of e-commerce?

As ASEAN documents refer to "e-commerce law(s)" or "e-commerce legislation," it is worth clarifying that these very terms may constitute sources of confusion. As indicated, the legal area most relevant to e-commerce is that of contract law and it remains debatable whether contract law requires any amendments to enable electronic transactions (see below) or whether the very concept of "e-

[21] Lao Law on Electronic Transactions, No 20/NA, 7 December 2012, Article 3.
[22] ASEAN Economic Community Blueprint 2025 (2015) p. 24; e-ASEAN Framework Agreement, Art. 5.
[23] UNCTAD Review; ASEAN Consumer Protection Digests and Case Studies: A Policy Guide (Volume I) (2014) Policy Digest 3: Consumer protection laws and regulations for online purchasing, p. 30-32.
[24] Michael Joachim Bonell, The CISG, European Contract Law and the Development of a World Contract Law, (2008) 56 *The American Journal of Comparative Law* 1.

commerce law" is warranted. While it could be argued that "e-commerce law" is, at its core, confined to contract law, it must be acknowledged that the term is often used more broadly, in reference to legal areas that are unrelated to the transactional aspects of e-commerce, such as e.g. domain names, intermediary liability or unsolicited commercial communications.[25] At the same time, however, contrary to what is implied by various ASEAN initiatives, one can hardly imagine that a single, all-encompassing law could address all legal issues *surrounding* online transactions. It seems more correct to speak of the "legal infrastructure" or "framework" for e-commerce because these terms expressly recognize the broad spectrum of challenges that must be addressed for e-commerce to flourish. Interestingly, despite broader declarations concerning the need for legal *frameworks* for e-commerce, ASEAN initiatives have centered on the enactment of electronic transaction legislation.[26] The realization that such instruments *by themselves* could do little to facilitate e-commerce seems of relatively recent origin.

2. The UNCTRAL Instruments – The Transactional Aspects of E-commerce

Two UNCITRAL instruments, the MLEC[27] and, more recently, the Convention on Electronic Contracting,[28] have been consistently promoted as a legal template for jurisdictions that have little or no e-commerce specific regulations. With a clear focus on contract, the UNICTRAL instruments prohibit any discrimination of contracts originating in electronic form and any disparity of treatment between electronic communications and paper documents.[29] These prohibitions are regarded as "enabling" e-commerce by removing doubts about the enforceability of contracts formed online. To date, multiple ASEAN jurisdictions have enacted domestic legislation based on either the MLEC or the Convention. For example, Malaysia has copied the provisions of the MLEC almost verbatim.[30] Singapore has adopted the modified wording of the Convention and added sections concerning electronic signatures, certification authorities and intermediary liability.[31] The Philippines substantially follow the MLEC but supplement their Electronic Commerce Act with multiple provisions governing specific aspects of online contracting, such as carriage of goods and transportation documents.[32] Indonesia's legislation addresses a wide range of issues related to the

[25] A good example is the Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ 2000 No. L 178, 17 July 2000, which combines multiple legal areas under the umbrella term "e-commerce."
[26] UNCTAD Review, p. 5-10.
[27] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment (1996) with additional article 5 *bis* as adopted in 1998.
[28] Convention on the Use of Electronic Communications in International Contracting, Nov. 23, 2005, U.N. Doc. A/60/21.
[29] MLEC Article 8, Explanatory Note, para. 129.
[30] Malaysia, Electronic Commerce Act 2006.
[31] Singapore, Electronic Commerce Act 2010, sections 18, 22 and 26.
[32] Republic Act No. 8792 of Philippines Electronic Commerce Act of 2000, for example section 16 (2) addresses electronic transactions made through banking networks, section 25 regulates actions relating to contracts of carriage of goods and section 26 deals with transportation documents.

digital economy, such as domain names and dispute resolution.[33] The provisions dealing with electronic transacting seem to follow the MLEC but, upon closer examination, reveal an idiosyncratic mixture of legal and technological misunderstandings.[34] Lao models the relevant sections of its e-commerce instrument on the MLEC,[35] but also includes multiple provisions on electronic signatures, dispute resolution and intermediary liability.[36] A similar approach is adopted in Myanmar,[37] Thailand,[38] Brunei Darussalam[39] and Viet Nam,[40] all of which follow (to a greater or lesser extent) the wording of the MLEC and add provisions governing other legal aspects of online transacting. It is worth observing that (a) the adoption of the MLEC in individual ASEAN jurisdictions is by no means uniform and that the relevant "electronic transactions acts" frequently address legal issues that are not directly related to the transactional aspects of e-commerce; and (b) to date, only Singapore and the Philippines have acceded to the Convention. Most pertinent to the present discussion is the fact that the choice of the MLEC as the baseline for e-commerce legislation appears doubtful.

(a) An outdated model?

The MLEC may be outdated and simply inadequate, leading to a situation where the laws modelled after its provisions may be unable to accommodate – not to mention facilitate – modern e-commerce transactions. The MLEC dates back to 1996, a time when e-commerce was in its infancy. During the preparatory works UNCITRAL did not review existing laws as to their ability to address technological change and did not wait for commercial practices to crystallize but concluded, in a broad-brush manner, that existing laws were inadequate to accommodate electronic transactions and that new laws were necessary. The instrument itself constitutes an adaptation of UNCITRAL's prior work relating to Electronic Data Interchange ("EDI"),[41] which refers to the automated exchange of structured data on the basis of *prior agreement* between sophisticated commercial entities communicating over closed, proprietary networks.[42] Principles deriving from such relationships can hardly serve as a template for legal instruments facilitating transactions in open, public networks between businesses and consumers, who have no prior dealings with each other. To aggravate matters, the drafters of the MLEC possessed a limited understanding of the technologies involved.[43] Many provisions prove, upon closer scrutiny, better suited to email, telex or static PDF files than to interactive websites or apps – not to mention such modern but prevalent online phenomena as

[33] Law of The Republic of Indonesia Number 11 of 2008 Concerning Electronic Information and Transactions, articles 23-26.
[34] see articles 17-22, particularly articles 21 and 22 seem to conflate problems of message integrity and problems of automation.
[35] Law on Electronic Transactions, No 20/NA, 7 December 2012, articles 8-12.
[36] Law on Electronic Transactions, No 20/NA, 7 December 2012, articles 40-45.
[37] The Electronic Transactions Law (The State Peace and Development Council Law No. 5/2004) art 21-29.
[38] Electronic Transactions Act B.E. 2544 (2001).
[39] Electronic Transactions Act 2008, Articles 11-15.
[40] Law on E-Transactions 51/2001/QH10 of 25/12/2001 of the 10 Legislature, Session No. 10;
[41] MLEC Guide to Enactment, p. 1.
[42] The Electronic Messaging Services Task Force, 'The Commercial Use of Electronic Data Interchange – A Report and Model Trading Partner Agreement' (1990) 45 *Business Law* 1645.
[43] Amelia Boss, 'The Evolution of Commercial Law Norms: Lessons To Be Learned From Electronic Commerce' (2009) 34 *Brooklyn Journal of International Law* 673, at 687.

transactions in information or the "sharing economy." Given that the MLEC (and hence the Convention) relies on an outdated understanding of e-commerce and given that online commercial practices have continued to evolve beyond EDI and email, ASEAN's promotion of these instruments seems unfortunate.

(b) Legal obstacles to electronic contracting?

The MLEC governs all electronic communications pertaining to the formation or performance of a contract.[44] Contracts have, however, never been regulated because of the manner they are formed. Contract law is generally indifferent to how the transacting parties communicate their intention. The UNICTRAL instruments imply, however, that many legal requirements prescribe the use of traditional paper documentation and thus impede the adoption of e-commerce.[45] Interestingly, such "legal requirements" are non-existent in contract law. Formalities, such as writing or signatures, are often required by statute[46] or by the contracting parties themselves. From the perspective of contract law – and the MLEC and the Convention purport to facilitate electronic *contracting* - the electronic form does not pose an obstacle to valid on-line transactions because contractual intention can be manifested in any manner,[47] including tweets or websites. It is, of course, acknowledged that some statutes or regulatory instruments may not be amenable to broad interpretations to accommodate dematerialized communications and hence require amendment or even replacement.[48] It is, however, necessary to distinguish between the need to update legislation from the need to update contract law. It is also necessary to differentiate between questions of substantive law and questions of evidence. Writing and signatures are, in most jurisdictions, not prerequisites of enforceability. They may, however, significantly facilitate proof of a transaction.

(c) A substantive interference?

Given that virtually all mass-market consumer transactions are devoid of any formalities, it is arguable that e-commerce transactions do not require a "removal of obstacles." If the UNCITRAL instruments were confined to confirming the enforceability of contracts formed online, they could be regarded as an attempt to alleviate any remaining concerns in this area. Unfortunately, the MLC and the Convention go further and introduce *substantive* provisions regarding online contracting. The latter create a discrete regime for e-commerce transactions that may differ from and interfere with the principles of contract law governing transactions formed by traditional means. For example, MLEC

[44] See: S. Eiselen, 'The Interaction between the Electronic Communications Convention and the United Nations Convention on the International Sale of Goods,' in A.H. Boss & W. Killian, eds., *The United Nations Convention on the Use of Electronic Communications in International Contracts* (Kluwer 2008) ("*Boss & Killian*"), p. 333-352

[45] MLEC Explanatory Note, para. 50.

[46] *See, e.g.*, Civil Law Act (Cap. 43) (Rev. ed. 1985) (Sing.)

[47] A. Phang, D. Seng Kiat Boon, Yeo Tiong Min, *The Impact of Cyberspace on Contract Law, Impact of the Regulatory Framework on E-Commerce in Singapore (2002)* ("Phang, Seng, Yeo"), at para 4, available at www.lawnet.com.; skeptical readers are invited to recall the last time they signed a document when making a purchase on amazon.com.

[48] T. Pistorius, 'Contract Formation: a Comparative perspective on the Model Law on Electronic Commerce,' (2002) 15 *Comparative & International Law Journal of South Africa* 129 at 130; Harry S.K. Tan, 'The Impact of Singapore's Electronic Transactions Act on the Formation of E-contracts,' (2002) 9 *Electronic Commerce Law Review* 85.

Article 10 determines when and where electronic communications are deemed to have been dispatched or received, thereby directly affecting the determination of the time of contract formation. Its wording is, however, not only technically inconsistent (due to UNCITRAL's failure to distinguish between various parts of the network infrastructure and its misunderstanding of the client-server model) but also more suitable to email than to web-based transactions, which dominate e-commerce. MLEC Article 14 introduces a complex provision governing acknowledgments of receipt that requires multiple exchanges of messages before a contract is deemed concluded. This mechanism may introduce legal uncertainty as to contractual communications, such as offers or acceptances, that have been received but remain unacknowledged. ASEAN jurisdictions that have adopted those provisions[49] will, inevitably, face difficulties in establishing the precise moment of contract formation. Traditionally, the legal principles governing the time of contract formation are formulated in broad terms that are amenable to different, case-specific interpretations. The MLEC, however, seems to impose a detailed and inflexible regime that may not be able adapt to constant technological change. For example, in Singapore, which is a common law jurisdiction, a contract is concluded when acceptance is *communicated* to the offeror or when the parties *reach* agreement.[50] In Thailand, which is a civil law jurisdiction, a "contract between persons at a distance comes into existence at the time when the notice of acceptance *reaches* the offeror."[51] In both instances, the terms "communicate" and "reach" can be interpreted to allow for various technologies. The MLEC provisions, however, associate the formation of a contract with, depending on the circumstances, electronic messages entering (a) "an information system outside of the control of the originator," (b) a "designated information system" or electronic messages being retrieved by the addressee. Given the broad definition of "information system" and the problems surrounding the concept of "designation," the said provisions are difficult to apply in practice as they replace a broad, flexible principle with one that is rigid and technically incorrect.[52] The preparatory works also reveal that UNCITRAL did not examine whether the substantive provisions introduced by the MLEC were compatible with existing principles or whether such existing principles could accommodate electronic transactions without legislative assistance. In sum, the introduction of substantive provisions in the MLEC (subsequently implemented in local electronic transaction acts) creates a parallel, incompatible and possibly redundant regime for contracts formed by electronic means.

3. Creating Trust: Digital and Electronic Signatures

[49] See e.g. Malaysia, Electronic Commerce Act 2006, Article 24; Philippines Section 20; Indonesia Article 20; Thailand Electronic Transactions Act B.E. 2544 (2001) Section 19.

[50] See generally: Andrew Phang Boon Leong, ed, *The Law of Contract in Singapore* (Singapore: Academy Publishing, 2012) Chapter 3.

[51] Thai Civil and Commercial Code, Section 361.

[52] For an in-depth discussion see: E. Mik, 'Certainty at Last? A "New" Framework for Electronic Contracting in Singapore' (2013) 8 *Journal of International Commercial Law and Technology* 160.

ASEAN initiatives, including both Blueprints as well as the e-ASEAN Framework, emphasize the need to enact laws regulating (and *promoting* the adoption of) electronic and digital signatures. Purportedly, the very success of e-commerce hinges on the widespread adoption and cross-border recognition of electronic and/or digital signatures. The latter are commonly promoted as a secure method of confirming the identity (i.e. authenticating) of the other party *and* as a functional equivalent of traditional signatures, which may be necessary to meet formal requirements. Unnecessary confusion, however, derives from an inconsistent use of terminology. "Electronic" signatures relate to any electronic representations of a name, such as those found on the bottom of emails, whereas "digital" signatures have a clear technical definition and rely on asymmetric cryptosystems.[53] Unfortunately, ASEAN initiatives refer to both terms interchangeably, creating a situation where regulatory proposals and existing legal instruments[54] require meticulous analysis to establish the underlying intent. To illustrate: the Blueprint 2025 directs ASEAN members to establish "inter-operable, mutually recognized, secure, reliable and user-friendly e-identification and authorization (electronic signature) schemes"[55] Such schemes are, however, difficult to envisage in relation to *electronic* signatures, which are only words on the screen and cannot be evaluated in terms of reliability or security. It is also difficult to imagine how names could be mutually recognized or inter-operable. It can be suspected that the Blueprint 2025 tried to remain technologically neutral while, at the same time, assuming that only *digital* signatures can facilitate e-commerce. Only the latter require cross-recognition or interoperability in the context of cross-border transactions (see below). This conclusion can also be reached in light of other ASEAN proposals.[56] To date, many ASEAN jurisdiction have enacted legislation addressing digital and electronic signatures, either as stand-alone instruments[57] or as part of their electronic transaction legislation.[58] It must be emphasized, however, that the focus on signatures may be misguided – at least when it comes to the purely transactional, commercial aspect of e-commerce.

3.1 Some common misunderstandings

ASEAN initiatives assume that e-commerce requires the ability to authenticate the other party. It is overlooked, however, that in traditional transactions parties rarely have an assurance that the other party is who he claims to be. The ability to authenticate is thus not an inherent characteristic of traditional transactions that must be preserved or re-created online. It is always the parties themselves who decide what level of trust they require and how much risk they were willing to assume. *How* and

[53] See generally: Bruce Schneier, *Applied Cryptography* (New York: Wiley, 1996) 34.
[54] See, e.g. the Vietnamese Law on E-Transactions (51/2005/QH11); Indonesian Law Concerning Electronic Information and Transactions, articles 11-16.
[55] ASEAN Blueprint 2025, p 24.
[56] See e.g. Reference Framework, paragraphs 14 and 15.
[57] See e.g. Malaysia, Digital Signature Act 1997
[58] See e.g. Singapore Electronic Transactions Act (2010).

whether the parties authenticate each other largely depends on the subject matter and value of the transaction. Authentication seems more important in cross-border transactions, particularly in case of delayed payment or when there is a risk of latent defects in the contractual subject matter. This does not mean, however, that the law should actively prescribe a specific authentication technology – especially before such technology is proven commercially viable.[59] Moreover, those who promote digital signature regulations assume that traditional signatures are indispensable for authentication and for contracting in general. This is incorrect. Signatures are generally not a method of authentication because they need not be legible or even biometrically related to the signatory. People are not identified by their signatures but by their government issued identification cards, drivers licenses or passports. Lastly, signatures are rarely a prerequisite of enforceability because contract law, as indicated, contains virtually no formal requirements.

3.2 Problems of authentication and the mutual recognition of signatures

ASEAN initiatives *incorrectly* assume that digital (or electronic) signatures are technically capable of authenticating the other transacting party. A brief technical explanation is necessary. Digital signatures rely on the mathematical correspondence between the private and the public key in asymmetric cryptosystems. For digital signatures to work, the public key must be accessible to everyone, the private key - exclusively to its authorized user. Multiple problems arise.

(a) Establishing a legal and technical infrastructure

A trusted third party must guarantee that a given key-pair belongs to a specific person. Consequently, digital signatures require a Certification Authority ("CA"), which manages the issuance of Digital Certificates ("DCs").[60] A DC contains information about the person it was issued to ("subscriber") and the public key. When issuing a DC, the CA must confirm the subscriber's identity.[61] If a CA does not correctly authenticate the potential subscriber, the digital signature is worthless because the subscriber can obtain the DC under a fictional name. It is, however, difficult to ensure that CAs in different jurisdictions are equally diligent in this process, particularly in the absence of common standards and procedures. It must be emphasized that each ASEAN jurisdiction has a *different* legal regime governing the establishment of CAs and the manner they issue DC.[62] In some ASEAN jurisdictions, like Lao or Myanmar, CAs are registered entities,[63] while in others, like Singapore,[64] their operation does not require a formal licensing regime. This raises significant problems when it

[59] This was the case with Directive 2000/46/EC on the taking up, pursuit of and prudential supervision of the business of electronic money institutions, which was repealed after 8 years as it stifled the development of e-money in the EU.
[60] Neil Ferguson, Bruce Schneier, *Practical Cryptography* (Indianapolis, Wiley 2003) p. 29.
[61] D. S. Anderson, 'What Trust is in These Times? Examining the Foundation of On-line Trust,' (2005) 54 *Emory Law Journal* 1441.
[62] Compare e.g. Singapore, which does not prescribe a licensing regime for CAs with Lao, which requires that CAs be authorized and registered with the relevant ministry, see: Lao Law on Electronic Transactions, No 20/NA, 7 December 2012, 26-29.
[63] Lao 28, Myanmar The Electronic Transactions Law (The State Peace and Development Council Law No. 5/2004) 12-18.
[64] Singapore Electronic Transactions Act 2010.

comes to the mutual recognition of digital signatures and cross-certification of CAs. These problems are illustrated in the Reference Framework, which describes the differences in the manner CAs are regulated in individual ASEAN jurisdictions.[65] For example, the Vietnamese Law on Electronic Transactions states that the Government recognizes the validity of foreign e-certificates and e-signatures if they are *equally reliable* as those that have been issued in accordance with Vietnamese laws.[66] In effect, the contracting parties from two different ASEAN jurisdictions would have to ensure that their digital signatures comply with the laws of their local jurisdiction *and* with the laws of the jurisdiction of the counterparty. Even if both parties adopted the highest common technological denominator, there would be no guarantee that their digital signatures will be recognized in the jurisdiction of the counterparty. The administrative and technical overhead accompanying cross-border transactions involving digital signatures issued in accordance with different standards and procedures will be impossible to bear – for both consumers and online businesses. The difficulties of cross-border certification and hence the mutual recognition of digital signatures are, however, generally underestimated. It is overlooked that such mutual recognition requires an intricate regulatory framework encompassing co-operating CAs and a comprehensive regional agreement addressing the technical standards of establishing CAs and issuing DCs.

(b) The "Private Key" problem

Digital signatures only guarantee that a message was "signed" with a specific private key. They cannot ensure that the key was used by the authorized person, i.e. the subscriber. The problem lies in securing the private key and preventing its unauthorized use. Given the frequency of network and device compromises, there is a high potential for private keys to be used by unauthorized persons. Consequently, any legal framework accompanying digital signatures must contain rules allocating liability for compromised private keys.[67] For the subscriber, the problem lies in safeguarding the private key and avoiding liability for its unauthorized use. For the party relying on a digital signature, the problem is that even a detailed examination of a DC (i.e. confirmation that the public key corresponds to the private key used in creating the digital signature) *cannot reveal who used the private key*. For example, the Vietnamese Law on Electronic Transactions obliges the subscriber, amongst others, to "have means to avoid the unauthorized use" of his private key and to ensure the integrity of the information of a DC.[68] The first requirement is nearly impossible to achieve from a technical standpoint, as it requires the subscriber to store the private key off-line, use sophisticated biometric access controls and have in-depth expertise of network security. The fulfillment of the

[65] Reference Framework paras 28-31, 54-57.
[66] Viet Nam, Law on E-Transactions 51/2001/QH10 of 25/12/2001 of the 10 Legislature, Session No. 10; Article 27.
[67] Jane Kaufman Winn, 'The Hedgehog and the Fox: Distinguishing Public and Private Sector Approaches to Managing Risk for Internet Transactions' (1999) 51 *Administrative Law Review* 955; also see Digital Signature Act 1997 (Malaysia) and ETA Singapore 2010, neither of which addresses liability allocation comprehensively.
[68] Viet Nam Law on E-Transactions, Article 25; *cf* section 43 of the Malaysian Digital Signature Act 1997, which provides that "the subscriber named in the certificate assumes a duty to exercise reasonable care to retain control of the private key and prevent its disclosure to any person not authorized to create the subscriber's digital signature."

second obligation largely depends on the reliability and responsiveness of the CA. The latter controls the DC and introduces updates to its contents, such as suspensions or revocations of DCs. The same instrument obliges the party relying on the "e-signature" to "verify its reliability" as well as the validity of the DC.[69] Again, the relying party is practically unable to verify either – unless we assume that he is to examine the technology underlying the specific digital signature, the manner it was deployed in a given transaction as well as the manner CAs issue DCs. The relying party always faces the risk that the subscriber will claim that his private key has been used without authorization. The presence of a CA changes nothing in this regard because the CA cannot control the security of private key. It can only represent to the relying party that the DC (and the key-pair) was *issued* in accordance with the relevant regulations and that it contains accurate information concerning the subscriber.[70] In practice, the use of digital signatures requires a great deal of technological sophistication on both sides of the transaction, specifically with regards to the ability to safeguard the PINs or passwords protecting the private keys.[71] Logically, such sophistication cannot be expected in jurisdictions where consumers lack basic experience with credit cards and online payments.

3.3 Lessons from other jurisdictions

ASEAN's continued promotion of digital signature laws is surprising given that, to date, such laws have proven unsuccessful. The first digital signature law, the Utah Digital Signature Act, was repealed in 2007.[72] Similarly, the EU Digital Signatures Directive,[73] which promoted digital signatures in a commercial context, has been replaced with a Regulation of a narrower scope that focuses on the cross-recognition and interoperability of national electronic identification schemes, predominantly in the context of public services.[74] The EU Commission found that private parties had not been using digital signatures in e-commerce transactions and that simpler electronic signature applications had become available.[75] It is also difficult to find a single jurisdiction where digital signatures contributed to the success of e-commerce.[76] Even in those ASEAN jurisdictions that have market economies, modern internet infrastructures *and* digital signature laws (Malaysia and Singapore), their use is virtually non-existent. In practice, problems of authentication and liability allocation are solved in a less technology-intensive manner. Most e-commerce vendors, such as

[69] Viet Nam Law on on E-Transactions, Article 26.
[70] This is exemplified by sections 34 and 36 of the Malaysian Digital Signature Act 1997.
[71] Theoretically, an effective digital signature scheme would require that *each use* of the private key relied on biometric access controls. Biometrics, however, raise multiple concerns, especially regarding the process of enrolment and the subsequent management of biometric data, biometric-based access controls can only function in closed organizations or in conjunction with existing government-controlled e-identity cards, see: A. Taipale, *Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd* (2004-2005) 7 Yale Journal of Law & Technology 123.
[72] UTAH CODE. ANN. §§ 46-3-101 (1999); the bill repealing the Utah Digital Signature Act was signed into law in 2006. S.B. 20, 2006 Leg., Gen. Sess. (Utah 2006).
[73] Directive 1999/93/EC on a Community framework for electronic signatures OJ 2000, No. L013, 19 January 2000.
[74] Regulation No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
[75] See Report on the Operation of Directive 1999/93/EC on a Community Framework for Electronic Signatures, 5.2, COM (2006) 120 final.
[76] Aside from being part of the https protocol, which creates secure connections between web-servers and clients.

amazon.com or Lazada.com, require the establishment of an account, which involves the consumer agreeing to standard terms and, quite often, the provision of payment information. The terms usually state that customers must protect their account information (e.g. password) and are liable for any activity originating therefrom. Individual purchases usually involve authentication mechanisms by the consumer's bank, which issued the credit card.[77] The liability for unauthorized transactions (and false identities) is apportioned by contract and partially absorbed by the financial institutions providing the payment infrastructure. It becomes clear that digital signatures are not an indispensable component of a legal framework facilitating e-commerce. Their use may be confined government-sanctioned authentication schemes enabling online interactions with public authorities, such as the electronic filing of tax returns. It is thus unfortunate that many legal instruments designed to enable e-commerce are dominated by provisions governing the establishment certification authorities.[78] ASEAN jurisdictions should de-emphasize the importance of digital signatures laws – at least in the context of B2C transactions. The focus should, instead, be placed on the development of secure online payment mechanisms. In mass-market consumer transactions, be they online or offline, identity seems less important than the ability to pay. The accompanying risks are usually spread amongst the financial intermediaries facilitating the transaction.[79] The facilitation of e-commerce should be associated with the introduction of regulations obliging banks and credit card companies to absorb the cost of unauthorized online transactions – not with the imposition of digital signatures.

4. **Other Areas**

Apart from enacting "enabling" legislation following the UNCITRAL model and assuring the mutual-recognition of electronic and/or digital signatures, the facilitation of e-commerce is increasingly associated with the establishment of adequate consumer and privacy protection regimes. [80] Both are regarded as legal instruments serving to increase confidence in online transactions. In many ASEAN jurisdictions consumer and privacy protections are, however, underdeveloped. Before proceeding, it is worth making some general observations pertaining to both areas. Optimally, all ASEAN jurisdictions should adhere to a similar set of principles: uniform frameworks in the areas of privacy and consumer protection would alleviate many concerns that consumers have in relation to cross-border transactions and, as described below, would positively affect the transfer of personal information between various ASEAN jurisdictions. The selection of an adequate reference model becomes all the more pertinent. Moreover, both consumer and privacy protections require a careful balancing exercise: the interests of online consumers must be weighed against the interest of online businesses, especially SME's, which

[77] An example of such scheme is Verified by Visa, which involves one time passwords sent to the consumer's mobile phone.
[78] See, e.g. the Myanmar Electronic Transactions Law (The State Peace and Development Council Law No. 5/2004) sections 12-18.
[79] See e.g. in the US, the Federal Reserve Board promulgated Regulation E (12 C.F.R. Part 205) to implement the EFTA pursuant to authority granted under 15 U.S.C. § 1693b. 15 U.S.C. § 1601 (1982); in the EU the Payment Services Directive 2 (2015/2366) governs unauthorized credit card transactions, including mobile and internet payments.
[80] Blueprint 2025 (2015), p. 13,

may be unable to bear a heavy burden of compliance. After all, both consumer and privacy protections usually involve the provision of certain information and area-specific mechanisms of redress. Aspirational declarations concerning the need to protect the interests of consumers in e-commerce must therefore be evaluated against the risk of excluding smaller, local online vendors, who may lack the resources to fulfill more stringent regulatory requirements. The facilitation of e-commerce is associated not only with empowering consumers but also with empowering online vendors, particularly local SMEs.

4.1 Consumer Protection

While ASEAN has undertaken some consumer protection initiatives,[81] many ASEAN jurisdiction have only rudimentary laws in this area.[82] The problem often does not lie in the lack of *e-commerce-specific* instruments, but in the lack of basic consumer protections *in general*, such as those concerning product safety or the prohibition of unfair commercial practices. For example, while Singapore and Malaysia have relatively comprehensive protective regimes,[83] Lao, Cambodia and Myanmar are only beginning to address basic consumer issues.[84] In many jurisdictions, the introduction of consumer protections in e-commerce must be preceded by the creation of fundamental protections in traditional transactions. Although ASEAN itself provides few if any guidelines in this area, there are multiple models that provide points of reference.[85] Due to space constraints, the following sections only address consumer protection *in e-commerce*, recognizing the idiosyncrasies of new transacting environment. While traditional consumer protections continue to apply online, there is a *greater* need for protection in e-commerce than in traditional transactions because online fraud and deception assume novel forms. Additional problems concern the information density and cognitive challenges inherent in the online environment. To date, only Malaysia has enacted regulations specifically tailored to online transactions.[86] It must also be noted that, regrettably, problems of consumer protections in e-commerce are often subsumed under consumer protection in telecommunication services or the narrow area of the right to Internet access.

(a) Providing information

[81] e.g. ASEAN Strategic Action Plan for Consumer Protection (ASCAP) was developed to elaborate on the consumer protection measures under the AEC Blueprint 2025.
[82] ASEAN Consumer Protection Digests and Case Studies: A Policy Guide (Volume I) (2014) Policy Digest 3: Consumer protection laws and regulations for online purchasing, p. 30-32; see also: D. K. Round & S. Zeljka, 'Globalisation and Consumer Protection in East Asia: Is It a Zero Sum Game?' (2003) 12 *Asian-Pacific Economic Literature* 39.
[83] Singapore, Consumer Protection (Fair Trading) Act 2004; Malaysia: Consumer Protection Act (CPA) 1999.
[84] see individual country reports in ASEAN Australia Development Cooperation Program Phase II (AADCP II) 'Roadmapping Capacity Building in Consumer Protection in ASEAN' (2011).
[85] See e.g. OECD Guidelines on Consumer Protection in the Context of Electronic Commerce (2000); United Nations Guidelines for Consumer Protection (2016) UNCTAD/DITC/CPLP/MISC/2016/1
[86] Malaysia, Consumer Protection Act 1999, Consumer Protection (Electronic Trade Transactions) Regulations 2012, which require the provision of basic information and mechanisms enabling the rectification of errors and the provisions of acknowledgement of receipt of orders placed online.

Consumer protection is usually associated with the provision of information, the assumption being that informed consumers can protect their interests and make better decisions. Regulatory efforts must, however, acknowledge that instruments based exclusively on the provision of information have had limited success[87] and that consumer protection must consist not only in furnishing information, but more generally, in enabling consumers to make choices and protecting them from misleading or deceptive practices. Consequently, assuming that basic substantive consumer protections are in place, e-commerce-specific instruments should ensure that information is provided in manner allowing for the special characteristics of the online environment.[88] This has been recognized by the US Federal Trade Commission, which addressed the difficulties of making effective online disclosures and emphasized the challenges of hypertext and information density.[89] After all, e-commerce is characterized by large amounts of information presented on increasingly smaller screens. The problem is particularly pertinent in the ASEAN, where consumers access the Internet predominantly via their mobile phones. FTC explained that, amongst others, a disclosure is effective only if presented in a manner that makes it 'clear and conspicuous.' It also acknowledged that many consumers might find it difficult to "discover" information if the latter is viewable only upon the activation of hyperlinks, or requires additional scrolling. Arguably, it is not only the idiosyncrasies of the online environment that must be allowed for but also the fact that many ASEAN consumers may be particularly vulnerable due to their limited familiarity with the Internet. It may thus be necessary to provide additional protections for more disadvantaged consumers, such as older people and children, or to those who have less experience in using the Internet.[90] As many consumers are unfamiliar with novel forms of misconduct, such as phishing or spamming, they are less able to protect themselves.[91] ASEAN initiatives should thus acknowledge that the mere provision of information may be insufficient. More pro-active educational efforts may be necessary.

(b) Accommodating technological change

In selecting a regulatory model for ASEAN initiatives for e-commerce-specific consumer protection, a useful legal framework can be found in the European Union. It combines information requirements with certain substantive rights on the side of online consumers and, most importantly, contains provisions capable of accommodating technological change. For example, EU consumers must be provided with detailed information about the product or service, as well as information about the trader to ensure that he is easily contactable.[92] Moreover, online traders must explain the technical

[87] Stephen Bainbridge, 'Mandatory Disclosure: A Behavioral Analysis' (2000) 68 *University of Cincinnati Law Review* 1023.
[88] United Nations Guidelines for Consumer Protection (2016) 15, 20.
[89] Federal Trade Commission, 'Dot.com disclosures: How to Make Effective Disclosures in Digital Advertising' (2013).
[90] United Nations Guidelines for Consumer Protection (2016) 7.
[91] Patrick Quirk and John A. Rothchild, 'Consumer protection and the Internet' in: Geraint Howells *et al* ed., *Handbook of Research on International Consumer Law* (Cheltenham: Edward Elgar 2011) 333, 335.
[92] Directive 2011/83/EU of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, OJ 2011, No. L 304/64, 22 November 2011, Articles 5, 6, 7, 8.

steps required to conclude the contract, provide technical means for identifying and correcting input errors and immediate acknowledgments of the receipt of online orders.[93] These protective requirements seem particularly important for less experienced online consumers. The terms governing a particular transaction must be accessible, provided in a manner allowing storage and reproduction[94] and written in understandable language.[95] EU consumers are also protected from unfair standard contract terms[96] as well as false and misleading advertising.[97] In addition, EU consumers have the right to withdraw from online contracts without penalty and without providing any reason.[98] The EU model can be regarded as the high benchmark of consumer protection, which may be difficult to follow in less developed ASEAN jurisdictions as it places a very high costs of compliance on online businesses. The right of withdrawal alone would encounter significant obstacles as it involves cross-border returns of goods. While it is unrealistic to copy the EU model in the ASEAN, some of its aspects should be borne in mind – particularly with regards to the requirements to explain the transacting sequence, to provide error correcting screens and order confirmations. Another EU instrument, the Directive on Unfair Commercial Practices ('UCPD'), departs from the traditional mechanism of providing information and seeks to enable consumers to make informed and *meaningful* choices.[99] To this end, it prohibits certain practices without any qualifications. For example, Article 5 contains a general prohibition of unfair commercial practices, practices that are contrary to the requirements of professional diligence, *and* materially distort or likely to materially distort the economic behavior of the average consumer.[100] A material distortion occurs when a practice impairs the consumer's ability to make an informed decision, 'causing the consumer to take a transactional decision that he would not have taken otherwise.'[101] The generality of Article 5 aims to ensure that the directive is 'future proof.' The UCPD also prohibits the provision of false information or correct information presented in a manner that deceives or is likely to deceive.[102] The said directive curbs abusive marketing and sales practices, associated with profiling and personalization techniques.

(c) Addressing disputes and complaints

Technology aside, a discrete set of challenges concerns the cross-border character of e-commerce. The latter should not facilitate fraud (given the ease of establishing a website as compared to a

[93] Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ 2000 No. L 178, 17 July 2000; Articles 5, 10 and 11.
[94] id., Article 10.
[95] Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ 1993 No. L 95/29, 21 April 1993; Article 5.
[96] id., Article 3.
[97] Directive 2006/114/EC of 16 December 2006 concerning misleading and comparative advertising, OJ 2006 No. L 376/21, 27 December 2006; Article 5.
[98] Directive 2011/83/EU of 25 October 2011 on consumer rights.
[99] Directive 2005/29/EC of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') OJ 2005, No. L149/22, 11 June 2005. ("UCPD")
[100] UCPD Articles 5, 8, 9.
[101] UCPD Article 2 (e).
[102] UCPD Article 6 and 7.

physical outlet) or otherwise enable online vendors to avoid liability due to the fact that consumers from different jurisdictions are less likely to sue. At a basic level, online vendors must obey the relevant laws and regulations of the jurisdictions where they are offering of their goods and services. It is also paramount to guarantee that consumers can seek redress in their home jurisdiction and rely on effective dispute resolution mechanisms. Apart from ensuring that consumers cannot be *contractually* bound to arbitrate or to sue in a remote forum, as is the case in the US,[103] it becomes necessary to create cheap, fast and efficient complaints-handling mechanisms and/or online dispute resolution frameworks.[104] It is widely accepted that the difficulties of cross-border enforcement can be alleviated by the introduction of online dispute resolution mechanisms, which could provide an accessible and low-cost method of obtaining redress.[105] ASEAN could benefit from instruments and proposals in other jurisdictions.[106] In addition to establishing active consumer protection agencies and promoting co-operation between them, ASEAN members should join the International Consumer Protection and Enforcement Network ("ICPEN"),[107] which is a platform for sharing consumer protection issues, including best practices and legislative reforms. Notably, the ICPEN encompasses an online initiative, econsumer.gov, aimed at educating consumers about scams and online abuses.[108] To date, the only ASEAN members who joined the ICPEN are Viet Nam and the Philippines. As the creation of consumer protection regimes remains surprisingly low on the agenda,[109] "interim" consumer protections could be achieved by means of educational efforts for both consumers and traders, rather than awaiting legislative solutions. Such efforts could, to an extent, enable consumers to better appreciate the risks inherent in online activities.

4.2 Privacy

As in the case of consumer protection instruments, space constrains prevent a comparative review of ASEAN privacy initiatives. The section below address only those aspects of privacy, which are directly relevant to e-commerce. To date, ASEAN has not proposed a single, uniform regime that could be used as a template by those jurisdictions that lack regulations in this area. There are also no international privacy agreements in Asia, which could impose obligations concerning the contents of

[103] The Federal Arbitration Act 9 U.S.C. § 2 provides that an arbitration agreement "shall be valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract;" *AT&T Mobility LLC v. Concepcion* 131 S. Ct. 1740 (2011).
[104] United Nations Guidelines for Consumer Protection (2016) 9. It is noteworthy that the ASEAN-Korea Brainstorming Meeting on Building a Regional Online Dispute Resolution System and Interagency Coordination Mechanism to Improve Consumer Protection in E-Commerce and the Training Workshop on Capacity Enhancement in Investigating and Handling E-Consumer Disputes were held from August 8-11 in Ho Chi Minh City, Viet Nam.
[105] Amy J. Schmitz, 'Building trust in ecommerce through online dispute resolution,' in John A. Rothchild, ed., *Research Handbook on Electronic Commerce Law* (Cheltenham: Edward Elgar 2016).
[106] See e.g. Directive 2013/11/EU on Alternative Dispute Resolution for Consumer Disputes, 2013 O.J. (L 165) 63; or the UNCITRAL Technical Notes on Online Dispute Resolution (2017).
[107] See: www.icpen.org
[108] See: www.icpen.org/staying-safe-online.
[109] See the ASEAN 'Strategic Action Plan For Consumer Protection (ASAPCP) 2016- 2025: Meeting The Challenges Of A People-Centered ASEAN Beyond 2015,' which sets out ASEAN's strategy for consumer policy over the next ten years (2016-2025) and sets the timeline for modernizing national consumer protection legislation for 2020 – 2025, Appendix.

privacy laws.[110] Consequently, the privacy frameworks (if any) in the respective ASEAN jurisdictions have been influenced by various instruments, such as the OECD privacy Guidelines and the European Union (EU) Data Protection Directive, and vary in scope, strength of enforcement and general recognition of the need to protect consumers online. At present, Cambodia, Myanmar, Brunei and Lao, have virtually no legal instruments aimed at safeguarding the privacy of their citizens.[111] Only the Philippines has a comprehensive privacy law that covers both the public and private sectors,[112] while Malaysia and Singapore have narrowly formulated laws covering most of their private sector.[113] Vietnam and Indonesia have sectoral laws governing only their e-commerce and consumer sectors.[114] Thailand's limited privacy protections apply only to the public sector.

(a) Privacy risks in e-commerce

The need for e-commerce-specific privacy protections must be seen against a broader background. The digital economy predominantly relies on advertising and abounds in what is best described as barter transactions involving the exchange of personal information for the right to access online resources.[115] Unsurprisingly, many e-commerce businesses are built exclusively around the collection and commercial utilization of the information generated by consumers during their online activities.[116] Although e-commerce is often associated with consumer empowerment deriving from increased access to market information and increased retail options, the ability to collect and *process* the consumers' personal information by means of sophisticated new technologies, such as predictive analytics, gives online businesses unprecedented transactional advantages.[117] The latter manifest themselves in the ability to influence or even manipulate online consumer behavior.[118] An example is "personalization," the customized, user-specific display of online content, where the consumer's personal information is used to discover his preferences *and* to determine the maximum price he can be charged. Personalization can thus lead to price steering and to price discrimination.[119] Consequently, *modern* privacy regulations must acknowledge the commercial value of personal information as well as the practical implications of its collection, processing and subsequent utilization.[120] The privacy principles that are relevant in the context of e-commerce concern restrictions on the manner online businesses are allowed to *collect, process and utilize* the personal

[110] Graham Greenleaf, *Asian Data Privacy Laws* (Oxford University Press 2014) 478.
[111] See generally Greenleaf, above at note 110.
[112] The Philippines Data Privacy Act 2012.
[113] Malaysia, Personal Data Protection Act 2010; Singapore, Personal Data Protection Act 2010.
[114] Vietnam, Law on E-Transactions of 2005, Law on Information Technology 2006 (No. 67/2006/QH11); Indonesia, 'Regulation of the Government of the Republic of Indonesia Number 82 of 2012 Concerning Electronic System and Transaction Operation' unofficial government English translation, implementing the Information and Electronic Transactions Law (No. 11 of 2008).
[115] J. Whittington, Ch. J. Hoofnagle, 'Unpacking Privacy's Price' (2012) 90 *North Carolina Law Review* 1328, 1331.
[116] For a basic explanation see: Richard Warner, Robert H. Sloan, 'Behavioral Advertising: From One-Sided Chicken to Informational Norms' (2012) 15 Vanderbilt Journal of Entertainment & Technology Law 49, 57-60.
[117] Bert-Jaaps Koop, 'Law, Technology and Shifting Power Relations' (2010) 25 *Berkeley Technology Law Journal* 973, 1012-1013.
[118] Neil M. Richards, Jonathan H. King, 'Three Paradoxes of Big Data' (2013) 66 *Stanford Law Review Online* 41, 42; Ira S. Rubinstein et al., 'Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches' (2008) 75 *University of Chicago Law Review* 261, 272.
[119] Tal Z. Zarsky, 'Mine your own Business!" Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion' (2002-2003) 2 *Yale Journal of Law & Technology* 55, 19-22.
[120] Ryan Calo, 'Digital Market Manipulation' (2014) 82 *George Washington Law Review* 995, 1034.

information of consumers, including the extent to which they are permitted to *share such information* with third parties, including entities located in foreign jurisdiction. All privacy instruments are characterized by a tension between the interests of the businesses that collect and utilize personal information for the purposes of e.g. direct marketing or profiling and the interests of online consumers (or "data subjects") whose personal information may be used to their disadvantage. Logically, it is more beneficial for e-commerce businesses (but less beneficial for consumers) to face fewer (if any) limitations on what information they are permitted to collect, how they are obliged to collect it and how they allowed to utilize it. A typical example are obligations to inform data subjects of the purpose of collection and the need to adhere to such purpose in the subsequent utilization of the personal information. In principle, the more specific the stated purpose and the more restrictions on the use of the information for other, secondary purposes, the better for the data subject but the worse for the online business. At a basic level, the strength of privacy protections in e-commerce can be measured by the difficulty of obtaining the consumers consent to the collection and utilization of his or her personal information, by the level of disclosure concerning the primary purpose of collection and the degree of leniency granted to businesses in utilizing the information for secondary purposes.

(b) Consent and notice (disclosure)

Most privacy regulations permit the collection, processing and use of personal information on condition that online consumers are *informed about* and *consent to* such practices.[121] A popular manifestation of this approach takes the form of privacy policies, which are presented alongside the terms of use placed on the bottom of most websites. Instruments relying on notice assume that given the opportunity to inform themselves, consumers will give their consent with the full realization of its implications. Such assumption is incorrect. Privacy protections based on notice and consent have proven generally ineffective,[122] if only for the reason that providing more information in an environment that already abounds therewith usually results in information overload and cognitive strain.[123] These shortcomings have been amply documented, especially with regards to the fact that the mere presence of privacy policies often creates a false sense of security leading consumers to take more risks with their information.[124] In addition, as consent to virtually any form of collection and processing need not be informed or express, it can be implied from almost any behavior, such as the continued use of a website. For example, the Singapore Personal Data Protection Act 2012 (the "PDPA") permits the collection, use or disclosure of personal data where consent is deemed.[125] Instruments that rely on consent but do not prescribe the manner of its expression or do not require

[121] See e.g. Singapore, PDPA 2012 Section 13; Philippines, Data Privacy Act 2012, Section 12; PDPA (Malaysia), s. 6; Vietnam, Law on E-Transactions of 2005, Article 46.
[122] Fred H. Cate, 'The Failure of Fair Information Practice Principles,' in Jane Kaufman Winn ed., *Consumer Protection in the Age of the Information Economy* (Farnham: Ashgate 2006) 341, 342.
[123] O. Ben-Shahar, *More Than you wanted to know: the Failure of Mandated Disclosure* (Princeton: Princeton University Press, 2014).
[124] L Brandimarte, et al, 'Misplaced confidences privacy and the control paradox' (2013) 4(3) *Social Psychological and Personality Science* 340.
[125] See PDPA Section 15.

explicit consent[126] can be interpreted broadly, leading to the same result as the PDPA. The resulting ease of obtaining consent renders many privacy protections ineffective, if not outright illusory. When creating e-commerce-specific privacy protections, is thus necessary to appreciate the limited effectiveness of instruments based on notice and consent. In this context, it is also necessary to acknowledge the significant differences between the EU, the US and the OECD approaches. The OECD and US prioritize the demands of the modern marketplace. For example, the OECD Guidelines,[127] which served as a template for privacy instruments in multiple jurisdictions[128] and also underlie the APEC Privacy Framework,[129] seem to limit the collection and uses of personal information but allow any such limitations to be overridden by notional notice and consent requirements. Interestingly, the recently updated OECD Privacy Framework recognizes the risks inherent in personalization techniques, [130] and the fact that consumers find it increasingly difficult to make informed choices related to their personal information. Nonetheless, it largely retains the principle that if online consumers are notified of the fact and purpose of collecting their personal information, online businesses can engage in the said activities without further restrictions.[131] Similarly, the US approach "substitutes" substantive limitations on the collection and processing of personal information with notice and consent requirements.[132] Despite different regulatory techniques, most ASEAN instruments permit the collection, processing and commercial utilization of personal information for virtually any purpose (including profiling) on condition that online customers receive certain information and provide their *implied* consent. On one hand, it could be claimed that this approach relies on a universally accepted and presumably adequate model. On the other, it must be acknowledged that the technological developments in the area of automated data processing and the accompanying ability to use the personal information of online consumers to *their* disadvantage, require a re-evaluation of any approach that places only minimal hurdles to such processing. Protections relying on consent and disclosure might have been sufficient in an ear where there less personal information was being collected and the subsequent utilization of such information was limited. Online businesses should permit their consumers, to the extent possible, to conduct their online activities anonymously or, if required, minimize the amount of information collected.[133] The subsequent use of personal information should be limited to its original purpose. Most importantly, online consumers should be protected from automated decisions that could affect their online and offline activities.

[126] see e.g. the Viet Nam Law on E-Transactions of 2005, Article 46(2) and the Philippines Data Privacy Act Section 12.
[127] OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data, OECD Doc. (C 58 Final) (1980)
[128] e.g. Australian Privacy Act of 1988; New Zealand Privacy Act of 1993.
[129] APEC Privacy Framework (2005); it is recognized that this framework offers only weak protections, see: Graham Greenleaf, 'APEC's Privacy Framework: A new low standard' (2005) 11 (5) *Privacy Law and Policy Reporter* 2004.
[130] OECD Privacy Framework (2013) 20, 66, 82, 83
[131] OECD Privacy Framework (2013), basic principles of national application 7, 8, 9, 10.
[132] The US has no single comprehensive system of privacy protection and relies on an inconsistent patchwork of federal and state laws, as well as self-regulatory measures. The Federal Trade Commission (FTC) only steps in when companies fail to self-regulate.
[133] Greenleaf, above at note 110, 486.

(c) Protections from automated processing

In selecting a model for privacy protections for e-commerce, it is worth considering the recently adopted EU General Data Protection Regulation ("GDPR").[134] The regulation specifically recognizes that the automated processing of personal information may result in profiling and economic discrimination.[135] While it does not expressly prohibit profiling, numerous provisions significantly limit its negative effects. For example, where personal information is processed for the purposes of direct *personalized* marketing, consumers have the right to object to such processing. Such right must be expressly brought to the consumer's attention and presented separately from any other information.[136] The GDPR requires that consumers receive specific information (presented in a clear and legible manner) about the purposes of processing and the presence and consequences of any profiling techniques. It also significantly restricts the processing of personal information for purposes other than those for which such information was originally collected.[137] Moreover, consumers have the right *not* to be subject to a decision based solely on automated processing, which significantly affects them. An example of such automated decision is the discovery or prediction of a person's preferences, interests or geographical location. [138] Profiling is only allowed where expressly authorized by law, e.g. for fraud and tax-evasion prevention, but also when necessary for the formation or performance of a contract, or on the basis of *express* consent.[139] The latter requires a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of agreement to the processing of personal information.[140] For consent to be informed, consumers must be made aware of the identity of the controller and the purposes of the intended processing. Consent is not freely given if, amongst others, the consumer has no genuine choice or is unable to refuse or withdraw consent without detriment,[141] if there is a clear imbalance between the consumer and the controller or if the performance of a contract is made dependent on consent despite it not being necessary for such performance.[142] In sum, the GDPR not only imposes tedious disclosure requirements and but also requires an enhanced act of consent, making it more difficult to override the substantive protections contained therein. Of course, in evaluating this approach ASEAN legislators will face the challenge of balancing the right of online consumers with the interests of online businesses – a challenge rendered even more difficult by the fact that less sophisticated online consumers will be unaware of their right to privacy and ignorant of the risks of automated data processing. While it is tempting to disclaim the GDPR as setting too high a standard in privacy protection, it must be acknowledged that adherence to such standard might be necessitated by the very

[134] Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ("GDPR").
[135] GDPR, Article 4 (4)
[136] GDPR, Article 21
[137] GDPR, Articles 5 and 6
[138] GDPR, Article 22, recital 71
[139] GDPR, Article 22
[140] GDPR, Article 4 (11) definition of "consent."
[141] GDPR, recital 42, Article 7.
[142] GDPR, recital 43.

fact that online consumers in less technologically advanced ASEAN jurisdictions may require more protection – persons unfamiliar with data mining and profiling techniques can hardly be expected to understand the relevant notices and provide their consent with a rudimentary appreciation of the implications of having their personal information processed and shared.

(d) A recent development – limitation of consent

In contrast to the EU, it is interesting to observe that in July 2017, the Singapore Personal Data Protection Commission ("PDPC") in Singapore conducted a "Public Consultation for Approaches to Managing Personal Data in the Digital Economy." It was recalled, amongst others, that the PDPA regards consent as the basis for collecting, using and disclosing personal data. While the PDPC acknowledged the technological advances and global developments in the areas of data processing, including Internet of Things devices, machine learning and artificial intelligence,[143] it suggested that such developments *challenge* consent-based approaches to privacy protection.[144] Arguably:

> *"Relying on consent requires lengthy notices that may not allow the individual to reasonably ascertain the purposes of the collection, use or disclosure of his or her personal data to provide meaningful consent. Individuals may become overburdened by the frequency of consent requests and the proliferation of lengthy consent clauses. The need to hold organizations accountable to act responsibly must be balanced with the need to address consent fatigue."*[145]

Instead of strengthening consent requirements to counterbalance the technological capabilities of online businesses, the PDPC proposed to permit the collection, use or disclosure of personal data *without consent* where it is necessary for a *legal or business* purposes.[146] It also considered that it may not be meaningful to *notify* individuals of the collection, use or disclosure for such purposes since, amongst others, such purposes may not be capable of specification at or before the time of collection. The Singapore proposal must be approached with caution. Admittedly, some individual consent decisions may not yield the most desirable collective outcomes (e.g. security threats) and some instances, such as legal proceedings, warrant a more liberal approach to consent requirements. In the context of *business* purposes, however, absolving commercial entities from obtaining consent can be regarded as extremely disadvantageous to consumers, further eroding their trust in e-commerce. A weakening of consent requirements in light of increasing technological capacities on the side of online businesses could only be excused by the introduction of substantive prohibitions concerning the processing of personal information – a mechanism conspicuously absent in the PDPC consultation.

[143] PDPC Consultation, p. 4.
[144] PDPC Consultation, p. 4.
[145] PDPC Consultation, p. 4.
[146] PDPC Consultation, p. 9.

(e) Restrictions on exports of personal information

It is logical to assume that there should be restriction on exports of personal information to jurisdictions which lack adequate privacy protections. Modern privacy instruments should thus specify the conditions in which exports of personal information are allowed, such as whitelisting the countries to which such information can be exported, providing contractual protections directly enforceable by the data subjects or imposing liability on data processors for the acts of parties the personal information was exported to. Unfortunately, it is also frequently implied that the modern, global economy requires uninhibited cross-border data flows leading to a situation where restrictions on personal data exports are often regarded with reluctance. The fact that unlimited data-flows between jurisdiction with differing protections might weaken or even annihilate the protections given to consumers in their local jurisdiction, is often overlooked. Greenleaf observes that existing ASEAN privacy laws contain very few restrictions on personal data exports,[147] to the point where data subjects in many jurisdictions need not even be informed of the fact that their personal information is exported. Interestingly, the adoption of more restrictive (i.e. consumer-oriented) privacy instruments may be negatively affected by the E-Commerce Chapter in the Trans-Pacific Partnership Agreement ("TPPA"),[148] which regards such instruments as trade barriers or discriminatory measures. Parties to the TPPA must allow the cross-border transfer of personal information to another jurisdiction for the conduct of an investor or service supplier's business, even if the latter lack adequate protections.[149] As a result jurisdictions with instruments favoring online consumers would be unable to protect their privacy by conditioning cross-border transfers of personal information on compliance with their privacy regimes.[150] The TPPA approach would, effectively, force ASEAN to adopt a regime least favorable to online consumers. The creation of a harmonized legal privacy framework seems thus even more important: if the protections accorded to online consumers are similar throughout the ASEAN, the imposition of export restrictions seems largely unnecessary.

5. Conclusions

Virtually all ASEAN e-commerce initiatives emphasize the scarcity of resources available to support efforts in this area. Going forward, it is necessary to ensure that such resources are used in the most efficient manner. To date, many initiatives can be regarded as misplaced or simply unnecessary. For example, instead of removing non-existent barriers to e-commerce in contract law or promoting the

[147] See Greenleaf, above at note 110, 500, 501.
[148] Trans-Pacific Partnership Agreement, Chapter 14, Electronic Commerce.
[149] Trans-Pacific Partnership Agreement, Chapter 14, Article 14.11.
[150] Although Chapter 14 permits exceptions to this principle but the exception seems difficult to use as it forces the relevant government to prove that it has a "legitimate public policy objective" and that such measure does not constitute a disguised trade restriction or discriminatory measure, see generally: Burcu Kilic & Tamir Israel, 'The Highlights of the Trans-Pacific Partnership E-commerce Chapter' (2015) at www.citizen.org/sites/default/files/tpp-ecommerce-chapter-analysis.pdf

use of digital signatures, governments and legislatures should focus on creating adequate consumer protection regimes and instruments safeguarding the online privacy of their citizens. An indiscriminate adherence to UNCITRAL instruments must be replaced with the recognition that the most successful jurisdictions in e-commerce do *not* rely on the MLEC. Many legal instruments in the area of e-commerce were premature and relied on untested assumptions as to their very necessity. It is commonly accepted that the law should *follow* not dictate commercial practice, so that it is necessary to exercise some restraint before such practices develop.[151] ASEAN jurisdictions lagging behind in the development of e-commerce laws may thus enjoy an unexpected advantage as their initiatives can be guided by mistakes made in other, purportedly more advanced jurisdictions. While it seems too late to reverse or repeal instruments based on the MLEC, it seems commendable to examine the extent the UNICTRAL instruments have actually facilitated the adoption of e-commerce. It is necessary to determine whether the creation of parallel legal regimes, one for traditional transactions and one for online transactions, is conducive to legal certainty. The differences between the legal systems in ASEAN jurisdictions should not be further enhanced by differences between online and offline transactions. It is also necessary to distinguish between the purely transactional aspects of e-commerce, which are generally governed by contract law, and such adjacent areas as consumer and privacy protection. Regulatory efforts must shift to the latter areas and focus on making the online environment safer for less technology-savvy consumers.

Although ASEAN initiatives emphasize the need to adopt "international standards," it must be observed that such standards may not exist. The United States, which can be regarded as the world leader in e-commerce, has a dramatically different legal landscape than the European Union, which is frequently regarded as lagging behind other jurisdictions, possibly due to the over-regulation of online transactions. Yet another legal framework exists in China, which is increasingly recognized as growing force in e-commerce and a standard-setter on its own. There is no single "international standard" that could serve as an aspirational target for regulatory initiatives aimed at facilitating e-commerce. It is also difficult to select a single ASEAN jurisdiction to serve as a model for other members. It is, however, possible to co-operate in order to establish which of the existing solutions adopted by individual ASEAN jurisdictions had a positive effect on the adoption of e-commerce. The fact that an ASEAN member has enacted laws in the relevant area does not imply, of course, that such laws are immutable and incapable of improvement. ASEAN member must maintain an open mind and learn from each other. It is also recommended to adopt a global view of the e-commerce environment and contemplate legislative and regulatory solutions from outside of the ASEAN. Moving forward, all ASEAN jurisdictions (both those that have privacy legislation and those that have shortcomings in this area) must re-evaluate their existing or planned instruments in light of technological progress and

[151] See: J. Zittrain, *The Future of the Internet* (Penguin 2008), who refers to such approach as the "procrastination principle," p. 119.

with a full appreciation of the risk inherent in automated data processing. E-commerce will only flourish if consumers can trust that their personal information is not misused or used against them. ASEAN initiatives should also refrain from formulating e-commerce-specific instruments in rigid or technology-specific terms, and aim to create laws and regulations that are capable of broad interpretations to accommodate the rapid and often unpredictable technological progress. Of equal importance is the acknowledgement that while the provision of information (be it in the context of consumer or privacy protection) is important, the special characteristics of the online environment must be allowed for in prescribing *how* such information is to be presented.

Additional developments in the area of e-commerce can be expected once the Regional Comprehensive Economic Partnership ("RCEP") is finalized.[152] Unfortunately, the RCEP negotiations are held in secret and the text of the e-commerce chapter is not publicly available. The limited resources indicate that the chapter will address, amongst others, paperless trading, electronic authentication, online consumer protection, the non-discriminatory treatment of digital products, customs duties on electronic transmissions and the online protection of personal information.[153] It is also worth mentioning that the TPPA Chapter on E-Commerce provides only rudimentary guidance in the area of e-commerce as its provisions are drafted in a broad manner and can be regarded as instructions as to *what* has to be done but not *how* it has to be done. For example, the Parties are directed to adopt consumer protection measures and to co-operate in this area.[154] There is, however, no mention of more specific principles or a recommended regulatory model. Moreover, most of the provisions of the Chapter on E-Commerce deal with areas that can be regarded as adjacent to e-commerce, such as customs duties, the non-discriminatory treatment of digital products or the promotion of competition in Internet access.[155] In sum, while ASEAN members must diligently observe any further developments with regards to the RCEP and the TPPA, it seems unlikely that these instruments will provide detailed guidance for the creation of e-commerce-specific instruments.

[152] The 20th Regional Comprehensive Economic Partnership (RCEP) Trade Negotiating Committee (TNC) meeting was held from 17 to 28 October 2017 in Songdo, Incheon, Korea. At present, it is expected that the RCEP will only be finalized in 2018.

[153] Regional Comprehensive Economic Partnership (RCEP) Negotiations, Discussion Paper on Electronic Commerce, May 2017, available at http://dfat.gov.au/trade/agreements/rcep/Pages/rcep-discussion-paper-on-electronic-commerce-may-2017.aspx

[154] See: Trans-Pacific Partnership Agreement, Chapter 14, Article 14.7.

[155] See: Trans-Pacific Partnership Agreement, Chapter 14, Articles 14. 3, 14.4 and 14.10