United Nations TD/B/C.II/EM.5/2

United Nations Conference on Trade and Development

Distr.: General
14 January 2015

Original: English

Trade and Development Board
Investment, Enterprise and Development Commission
Expert Meeting on Cyberlaws and Regulations for Enhancing E-commerce, Including Case Studies and Lessons Learned
Geneva, 25–27 March 2015
Item 3 of the provisional agenda

Cyberlaws and regulations for enhancing e-commerce: Case studies and lessons learned

Note by the UNCTAD secretariat

Summary

Electronic transactions are of growing importance to Governments, enterprises and consumers in most parts of the world. While greater reliance on electronic commerce (e-commerce) creates significant opportunities, a lack of security and trust remains a critical barrier to such transactions. Online fraud and data breaches are growing concerns requiring adequate legal and regulatory responses to boost domestic and cross-border trade. However, adopting an appropriate legal and regulatory framework is made difficult by the variety and complexity of cyberlaws and regulations as well as the rapid evolution of technologies and markets. New payment solutions and growing reliance on cloud computing accentuate the need for making progress in this area.

Against this background, this note examines key legal issues that need to be addressed to facilitate e-transactions and to make interaction on the Internet more secure in general. The note briefly reviews selected best practices in addressing commonly known challenges to the preparation and enforcement of cyberlaws based on UNCTAD's interaction with regional groupings in developing countries. It also presents the results of UNCTAD research into the current state of e-commerce laws in these areas, highlighting progress made and remaining gaps. It discusses possible options for achieving effective implementation and enforcement of the relevant laws taking into account the emergence of new technologies available on the Internet and mobile platforms. Policy actions should address the need for compatible laws and the building of capacities of key stakeholders, notably enforcement authorities.

GE.15-00469 (E)
1500469

Please recycle

Contents

		Page
I.	Introduction	3
II.	Global trends in e-commerce	3
III.	Key legal issues in e-commerce	6
	A. Implementing compatible e-signatures and e-contracts laws	7
	B. Protecting consumers online	8
	C. Addressing data protection and privacy online	10
	D. Fighting cybercrime	11
	E. Selected examples of best practices at the regional level	13
IV.	Recommendations and issues for discussion	14

I. Introduction

1. Given the transformational developments in the area of information and communications technology (ICT), in particular the emergence of the Internet in the second half of the 1990s and more recently the widespread use of mobile technology, there is growing recognition of the implications of ICT for trade and sustainable development. One important application of ICT is in the area of e-commerce.

2. Until recently, e-commerce uptake in many countries was hampered by various factors. Main barriers to e-commerce include inadequate ICT and electricity infrastructure, undeveloped financial markets, low purchasing power, low levels of ICT literacy and of awareness of e-commerce among consumers and enterprises, and weak legal and regulatory frameworks. Such barriers have been the most pronounced in low-income countries and among small enterprises and microenterprises.

3. In the light of new technologies, new e-commerce platforms and payment solutions, some of the above-mentioned barriers have become somewhat easier to overcome. This makes it important for Governments of developing countries to create enabling frameworks that allow enterprises and Governments themselves to take full advantage of opportunities for e-transactions using various ICT devices. Online fraud and data breaches are of growing concern for both consumers and enterprises, requiring adequate responses at national and international levels.

4. This note has been prepared in view of the terms of reference agreed upon for the expert meeting, which should focus on "relevant areas of consumer protection such as credit card and payment data protection and payment regulations…[with due regard] to complementary work undertaken in the WTO in the framework of the Work Programme on E-Commerce". The terms of reference further stipulate that the "expected outcome…would be the identification of best practices concerning cyberlaws and regulations on e-commerce as well as recommendations on ways of enabling the regulatory framework, including cyberlaws, for enhancing e-commerce".

5. The note draws on research conducted for the *Information Economy Report 2015* (UNCTAD, 2015) and concentrates on four legal areas: e-transactions, consumer protection, privacy and data protection, and cybercrime. It first presents recent global developments in e-commerce. It then identifies the main legal concerns that need to be addressed to enable e-commerce growth in developing countries and globally. Several brief case studies and best practices are highlighted, based on UNCTAD's work in developing regions, such as those of the Association of Southeast Asian Nations (ASEAN), the East African Community (EAC), the Economic Community of West African States (ECOWAS), the Sistema Económico Latinoamericano y del Caribe and the Asociación Latinoamericana de Integración. Finally, the note proposes selected issues and recommendations for experts to consider in the meeting.

II. Global trends in e-commerce

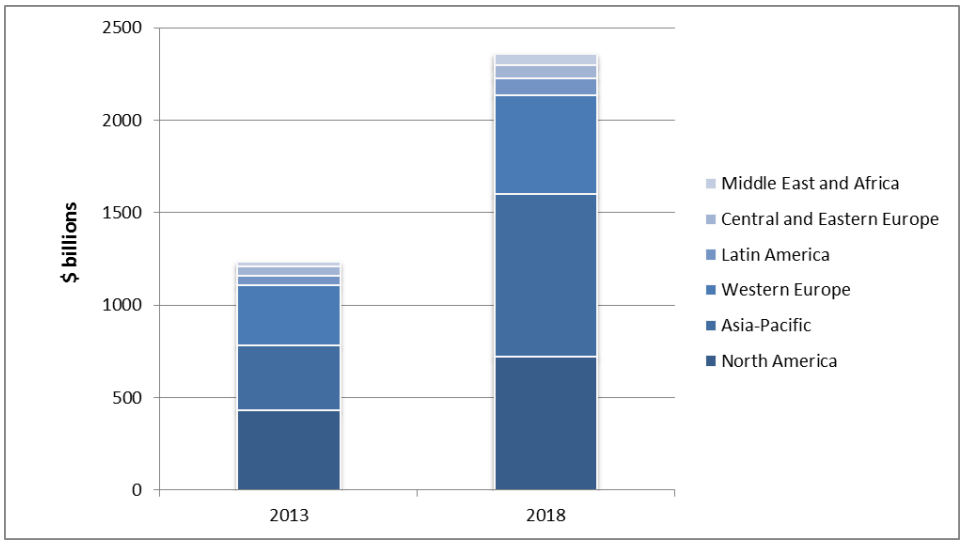
6. E-commerce offers potential benefits in the form of enhanced participation in international value chains, increased market access and improved efficiency, as well as lower transaction costs. However, the uptake of e-commerce in most developing countries has been slow and was for a long time confined to relatively few economies and enterprises (UNCTAD, 2010a).

7. From having been a phenomenon mostly reserved for large enterprises in developed countries, changes in the ICT landscape are creating greater opportunities for businesses in

developing countries to engage in various forms of e-commerce (UNCTAD, 2015). The connectivity situation has greatly improved, notably as a result of the widespread uptake of mobile telephony and social media. Moreover, new applications, platforms and services are making e-commerce more accessible and easy to navigate, thereby lowering the barriers to entry. New payment solutions similarly provide a wider choice for both enterprises and consumers to conduct transactions online. More e-commerce companies are appearing in developing countries, with offers that are tailored to the needs and demands of local users, helping to raise awareness among enterprises and consumers of online commerce.

8. Business-to-business transactions account for the overwhelming share of e-commerce revenue. They involve transactions between manufacturers and wholesalers, or between wholesalers and retailers. UNCTAD estimates that global business-to-business revenue amounted to $15.2 trillion in 2013, compared with $1.2 trillion in the case of business-to-consumer (B2C) transactions (UNCTAD, 2015). The latter type of transactions, which involve sales by "pure play" e-commerce enterprises to consumers and by traditional bricks-and-mortar retail or manufacturing firms that add an online sales channel, appear to be growing faster. According to e-Marketer, B2C sales are forecast to reach $2.4 trillion by 2018 (figure 1). The highest growth is expected in the Asia–Pacific region, the market share of which is set to grow from 28 to 37 per cent. The only other region that is forecast to increase its share of the global market is the Middle East and Africa, expected to grow from 2.2 to 2.5 per cent. Conversely, the combined share of Western Europe and North America is expected to fall from 61 to 53 per cent.

Figure 1
B2C e-commerce sales worldwide, by region, 2013 and 2018 ($ billions)



Source: eMarketer.com, July 2014.

Note: Data include products and services ordered and leisure and unmanaged business travel sales booked using the Internet via any device, regardless of the method of payment or fulfilment.

9. An estimated 1.1 billion people made at least one online purchase in 2013, accounting for just over 40 per cent of all Internet users (table 1). With some 460 million online shoppers, Asia–Pacific accounts for the largest share (43 per cent), a proportion that is expected to rise further until 2018. The fastest growth between 2013 and 2018 is anticipated for the Middle East and Africa.

Table 1
Digital buyers worldwide, by region, 2013 and 2018

	Total (millions)		*Growth 2013–2018 (%)*	*Share of world total of digital buyers (%)*	*Digital buyers as a share of population (%)*	*Digital buyers as a share of Internet users (%)*
	2013	*2018*		*2013*	*2013*	*2013*
Asia–Pacific	460.3	782.4	70	42.6	14.9	42.1
Western Europe	182.3	210.2	15	16.9	49.0	64.0
North America	172.3	203.8	18	16.0	59.7	72.0
Africa and the Middle East	93.6	170.6	82	8.7	7.1	31.3
Latin America	84.7	139.3	64	7.8	18.6	28.2
Central and Eastern Europe	86.4	117.4	36	8.0	24.1	41.6
World	**1 079.6**	**1 623.7**	**50**	**100.0**	**15.2**	**41.3**

Source: eMarketer, July 2014.

10. Credit cards account for the lion's share of retail e-commerce settlements (WorldPay, 2014). However, by 2017, other payments are expected to make up for the majority (59 per cent) of all retail e-commerce payments, with "e-wallets" representing more than 40 per cent of the total. The usage patterns vary greatly by region (table 2). In North America and Europe, credit cards remain the main method followed by e-wallets. Among developing countries, there is significant variation, but credit cards generally account for less than half. In Africa and the Middle East, cash on delivery is used in almost half the value of e-commerce transactions, partly reflecting a high proportion of unbanked people. In India as well, such payments still account for 50–80 per cent of all online transactions. Reliance on cash on delivery can act as an inhibitor of e-commerce growth due to people not paying when the product is delivered and to the lag between product dispatch and payment.

11. Mobile payments accounted for only 1 per cent of the value of e-commerce payments, a figure forecast to rise to 3 per cent by 2017. But they are more important in countries characterized by limited Internet use but well-functioning mobile money systems. In several African countries, mobile solutions represent the most viable infrastructure for e-services due to high degrees of financial exclusion, limited availability of fixed lines, cost of fixed lines and cost of the card infrastructure (Innopay, 2012).

Table 2
E-transactions value, by payment method and by region, 2012 (per cent)

Region	*Credit cards*	*E-wallets*	*Direct debit*	*Cash on delivery*	*Bank transfer*	*Other*
United States of America and Canada	71	18	2	1	1	7
Europe	59	13	5	5	8	11
Latin America	47	10	4	8	13	18
Asia and the Pacific	37	23	1	11	14	14
Africa and the Middle East	34	5	0	48	3	10
World	57	17	2	5	7	12

Source: WorldPay, 2014.
Note: Mobile payments included in "other".

III. Key legal issues in e-commerce

12. An adequate and supportive legal environment is essential to create trust online and to secure electronic interactions between enterprises, consumers and public authorities. The extent to which regions and countries have adequate legislation in place, as well as whether such legislation is effectively implemented and enforced, varies considerably. UNCTAD research shows that the availability of relevant laws in four legal areas that are essential for increasing users' confidence in e-commerce – e-transaction laws, consumer protection, privacy and data protection, and cybercrime – is generally high in developed countries, but inadequate in many other parts of the world (table 3).

Table 3
Share of economies with relevant e-commerce legislation, by region, 2014 (per cent)

	Countries (number)	*E-transactions laws (%)*	*Consumer protection laws (%)*	*Privacy and data protection laws (%)*	*Cybercrime laws (%)*
Developed economies	**42**	**97.6**	**85.7**	**97.6**	**83.3**
Developing economies					
Africa	**54**	**46.3**	**33.3**	**38.9**	**40.7**
Eastern Africa	**18**	38.9	16.7	27.8	50
Middle Africa	**9**	22.2	22.2	22.2	11.1
Northern Africa	**6**	83.3	33.3	50	66.7
Southern Africa	**5**	60	40	20	40
Western Africa	**16**	50	56.3	62.5	37.5
Asia and Oceania	**48**	**72.9**	**37.5**	**29.2**	**56.3**
Eastern Asia	**4**	75	50	25	50
South-Eastern Asia	**11**	81.8	81.8	54.5	72.7
Southern Asia	**9**	77.8	22.2	44.4	66.7
Western Asia	**12**	91.7	33.3	25	58.3
Oceania	**12**	41.7	8.3	0	33.3
Latin America and the Caribbean	**33**	**81.8**	**54.5**	**48.5**	**63.6**
Central America	**8**	75	87.5	37.5	37.5
South America	**12**	83.3	75	66.7	75
Caribbean	**13**	84.6	15.4	38.5	69.2
Transition economies	**17**	**100**	**11.8**	**88.2**	**70.6**
All economies	**194**	**74.7**	**47.4**	**55.2**	**60.3**

Source: UNCTAD.

A. Implementing compatible e-signatures and e-contracts laws

13. A prerequisite for conducting commercial transactions online, including electronic payments, is that there is legal equivalence between paper-based and electronic forms of exchange, which is the goal of e-transactions laws. E-transactions laws have already been adopted by 143 countries, of which 102 are developing countries (UNCTAD, 2015). Another 23 have produced draft legislation in this area. That leaves nine developing countries with no e-transactions laws and 18 for which data are lacking. While four out of five countries in Asia and in Latin America and the Caribbean have adopted such laws, Eastern and Middle Africa countries are lagging behind the most.

14. Many national laws in this area have been influenced by the legislative standards prepared by the United Nations Commission on International Trade Law (UNCITRAL). Its Model Law on Electronic Commerce (1996) (UNCITRAL, 1999) has been enacted in more than 60 jurisdictions. Meanwhile, 29 jurisdictions have based their legislation on the UNCITRAL Model Law on Electronic Signature (2001) (UNCITRAL, 2002). Meanwhile, the United Nations Convention on the Use of Electronic Communications in International Contracts has been signed by 18 States and acceded to or ratified by six (UNCITRAL, 2007). The Convention applies only at the international level, and only to the six States which are parties. However, several States have incorporated some or all of the substantive provisions of the Convention in their national laws.

15. Jurisdictions that have adopted the model laws or the Convention on the Use of Electronic Communications in International Contracts share common elements in their electronic contracting laws, helping to facilitate cross-border e-commerce. They embrace the principles of technology neutrality, non-discrimination of electronic communications and functional equivalence. But despite progress in the adoption of e-transactions laws, three main issues remain.

16. First, several e-transactions laws address only the electronic signature (e-signature) component (authentication) but are silent on other important contractual terms, such as time and place of dispatch and receipt, acknowledgment of receipt, party location and use of automated message systems. Similarly, most e-transactions laws do not deal with international aspects of e-commerce, such as choice of law, which is one of the potential issues of conflict in cross-border e-commerce. Moreover, while several laws have a provision on cross-border recognition of e-signatures, in many cases the provision is not implemented as it requires a system for mutual recognition to be put in place that is burdensome (Castellani, 2010).

17. Second, there is variation in terms of national implementation of fundamental principles, notably technology neutrality in the use of e-signatures. Some countries have enacted technology-specific legislation based on e-signatures, such as public key infrastructure. This applies, for example, to some member States of the Commonwealth of Independent States and of the Economic Community of West African States (ECOWAS). Commonwealth of Independent States member States are required to set up certifying bodies that create digital signatures based on cryptography. Some laws envisage that only these digital signatures be recognized as having a mandatory force. However, there may be a trend towards more technology-neutral laws. For instance, the Russian Federation in 2011 amended its law to recognize all forms of e-signatures and it also adopted the Convention on the Use of Electronic Communications in International Contracts, which enables cross-border recognition of e-signatures on a technology-neutral basis.

18. Furthermore, laws may require the establishment of a national certification authority. However, due to the human and financial costs involved, certification authorities, especially in developing countries, have sometimes not been set up, or have been set up

only after an extended period of time. In such cases, e-transactions may lack legal recognition when the intervention of the national certification authority is required to give legal validity to the transaction. In addition, a requirement to use cryptographic systems when conducting e-commerce or e-government operations can represent a barrier to online transactions. It could, for example, hinder foreign bidders to participate in public procurement, unless legal recognition of the relevant foreign public key infrastructure has been established.

19. Even in countries that have adopted provisions based on UNCITRAL or other uniform texts, variations exist, posing challenges for both domestic and cross-border e-commerce. Different e-transactions laws provide different standards for what constitutes an e-signature. The case of the European Union is illustrative. Its member States were required to implement the European Union Directive 1999/93/EC on a Community Framework for Electronic Signatures, which established the legal framework for e-signatures and certification services to be legally recognized within and across European Union member States. As the national regimes adopted to implement the Directive were not harmonized, the European Parliament and the Council of the European Union in July 2014 adopted the Regulation on Electronic Identification and Trust Services for Electronic Transactions. This Regulation applies the principle of technology neutrality by avoiding requirements that could only be met by a specific technology. It also sets conditions for mutual recognition of electronic identification in a legal instrument that is directly applicable in all European Union member States. Another example is ASEAN, in which member States recognize different types of signatures (UNCTAD, 2013a).

20. The third issue concerns the lack of capacity regarding the enforcement of e-transactions laws. Judges and practitioners often have limited knowledge of and experience with e-transactions. As a result, and especially in developing countries, companies may be reluctant to embrace the use of electronic means.

B. Protecting consumers online

21. Consumer protection seeks to address imbalances between businesses and consumers in all forms of commerce. Given the nature of the Internet, where important information on the seller (such as identity, location and credibility) can easily be concealed, this imbalance is accentuated in the case of e-commerce. Consumers are more vulnerable online to deceptive and fraudulent activities. Consumer protection laws can also help businesses engaged in e-commerce to clarify the requirements of doing business online within a particular jurisdiction. Therefore, consumer laws, policies and regulations may both outline consumers' rights and business practices that are to be expected online, limit fraudulent and misleading commercial conduct and help business develop self-regulatory regimes (Organization for Economic Cooperation and Development (OECD), n/d).

22. Despite the importance of consumer confidence for B2C e-commerce, the global mapping of consumer protection legislation indicates that many developing and transition economies still lack relevant laws (UNCTAD, 2015). Out of the 119 countries for which data are available, 90 (of which 56 are developing or transition economies) have adopted consumer protection legislation that relates to e-commerce. For as many as 73 countries, it was not possible to obtain data, however, possibly suggesting that consumer protection online has not been fully addressed.

23. In terms of regional patterns, the incidence of consumer protection legislation in Africa is particularly low. Only 18 of the 54 African countries have adopted such laws. The coverage is higher in Latin America with 16 out of the 20 countries in the region having relevant legislation in place. For Oceania and most transition economies, data on the state of consumer protection legislation is unavailable.

24. It is important to ensure that online shoppers are protected for both domestic and cross-border purchases. Differences in the way countries adopt relevant provisions can hamper cross-border transactions. These differences may be related to the rights and obligations of consumers and businesses, to what is to be considered acceptable terms and conditions, to disclosure obligations and effective international redress mechanisms.

25. In the European Union, for example, enterprises have to operate with 28 different sets of national rules for conducing cross-border trade. They therefore need to identify the provisions of the applicable laws of particular countries, and assume the costs associated with translation, legal advice and adaptation of contracts. This adds costs, complexity and legal uncertainty. In a 2011 survey of cross-border online trade, 44 per cent of consumers said that uncertainty about their rights had discouraged them from buying from another European Union country. A third of the consumers surveyed said they would consider buying online from another European Union country if uniform European rules applied, but only 7 per cent did (European Commission, 2011). To remedy this situation, the European Commission has proposed a Common European Sales Law to Facilitate Cross-Border Transactions in the Single Market.[1] This would give traders the choice to sell their products to citizens in another member State on the basis of a single set of contract law rules which would stand as an alternative alongside the national contract laws. Parties to a cross-border sales contract anywhere in the European Union would be able to choose, by express agreement, to apply the Common European Sales Law.

26. The cross-border enforcement of consumer protection is another challenge, requiring effective cooperation between the national enforcement agencies.[2] Some national authorities have set up semi-formal cooperation mechanisms and networks to serve as non-legal, political channels of cooperation. For example, the International Consumer Protection and Enforcement Network (ICPEN) is a network of public authorities involved in the enforcement of fair trade practice laws and other consumer protection activities, comprised of 56 member countries and organizations including 24 developing countries.[3] Its main objective is to identify ways to prevent and redress deceptive marketing practices in an international context.

27. The International Consumer Protection and Enforcement Network has developed the econsumer.gov initiative to enhance consumer protection and consumer confidence in e-commerce. The website invites individuals to file complaints online at a single location (http://www.econsumer.gov). As of 2014, it comprised 30 national authorities, all of which are also ICPEN members. In 2013, the initiative received 23,437 complaints, many of which related to cross-border transactions.[4]

28. The main international reference framework for the protection of consumers online is the Guidelines for Consumer Protection in the Context of Electronic Commerce (OECD Guidelines) (OECD, 2000) which are being revised. The objective of the revision is to reflect relevant policy principles pertaining to B2C e-commerce in a number of OECD Acts since their adoption in 1999. As they are updated for OECD member States, some developing countries may see a need to adapt the content of OECD Guidelines to domestic needs.

[1] Available from http://eur-lex.europa.eu/legal-content/en/ALL/;ELX_SESSIONID=9kq3JrXb6922fTl6wCNCyJTyMZn3N6p8lYymnk4b9G32fR21QJhQ!715408534?uri=CELEX:52011DC0636 (accessed 5 January 2015).

[2] This has been stressed by delegates within ASEAN and in Latin America in the context of UNCTAD's assistance; see, for example, UNCTAD (2013a).

[3] See https://icpen.org/ (accessed 5 January 2015).

[4] See http://www.econsumer.gov/english/resources/trends.shtm (accessed 5 January 2015).

29. At the global level, the United Nations is also conducting consultations on the revision of the United Nations Guidelines on Consumer Protection (UNCTAD, 2001) in the light of market and regulatory developments, including those related to e-commerce. The consultations aim to capture the needs of developing countries. The revised guidelines may be available by 2016. Salient topics discussed during the consultations include: effective protection that is no less favourable to that of other forms of commerce; rights and obligations of consumers and businesses; vulnerable consumers; mobile platforms; payment; alternative dispute resolution; consumer education and awareness; data and privacy protection; applicable law and jurisdiction; and bilateral, regional and international cooperation.

C. Addressing data protection and privacy online

30. In the global digital economy, personal data have become the fuel driving much commercial activity online. Every day, vast amounts of information are transmitted, stored and collected online, enabled by improvements in computing and communication power. In this environment, security of information is of growing concern to Governments, enterprises and consumers alike. The surge in cloud services provided across jurisdictions, and the growing number of data breaches accentuate the need for adequate policy responses (UNCTAD, 2013b). Analyses of "big data" aimed at understanding and influencing consumer behaviour for commercial profit may further exacerbate such concerns.

31. According to one source, more than 2,100 incidents were reported in 2013, through which some 822 million records were exposed (Risk Based Security, 2014). In one major incident, as many as 152 million names, customer identities, encrypted passwords, debit or credit card numbers and other information relating to customer orders were exposed. The business sector was the target for 53 per cent of the incidents, followed by Governments (19 per cent). About 60 per cent of the incidents were the result of hacking.[5] In terms of geographical patterns, the United States was by far the most targeted country, accounting for almost half of the known cases. The most common types of data exposed were passwords, names, e-mails and user names.

32. As of November 2014, 105 countries (of which 65 developing countries) had put in place legislation to secure the protection of data and privacy (UNCTAD, 2015). Another 34 developing countries had draft bills pending enactment. In this area, Asia and Africa have a similar level of adoption, with less than 40 per cent of countries having a law in place.

33. Companies also need to adopt policies to keep information secure, put in place technical safeguards, and develop response plans for data security incidents, as well as to avoid fraudulent, deceptive and unfair practices. In view of the nascent stage of privacy and data protection laws in sub-Saharan Africa, some e-commerce companies have proactively adopted international best practices and security standards (box 1). Where privacy and consumer protection is difficult to guarantee due to the nature of the content model, service providers may need to take extra measures to educate buyers and sellers on how to recognize and protect themselves from fraud.

[5] "Hacking" here refers to the gaining of access (wanted or unwanted) to a computer and viewing, copying, or creating data (leaving a trace) without the intention of destroying data or maliciously harming the computer.

Box 1. Company responses to data protection and privacy in East Africa

In emerging e-commerce in sub-Saharan Africa, data breaches have thus far been largely offline automated teller machine and point of sale terminal fraud. There have been incidents of skimming devices that record a payment card's details. Online fraud also occurs, and its prevalence will only increase as more and more consumers come online. Several e-commerce marketplaces have put in place mechanisms to handle the risk of fraud.

OLX, an online classifieds site present in Kenya and many other countries, adheres to the Safe Harbour Privacy Principles of notice, choice, onward transfer, security, data integrity, access and enforcement. In its terms of service, it outlines how data are collected, used and shared as well as what measures are taken to protect an individual's data. If users suspect that their privacy has been violated or otherwise compromised, OLX encourages them to report the issue using OLX's "legal issues report form".

3G Direct Pay is an e-commerce payment gateway that serves over 300 travel and tour operators throughout East Africa. It approaches data security in much the same way as a bank. As a card processor, it handles sensitive payment card data that, if stolen, can be used to initiate card payments without the card owner's consent. To mitigate this, 3G Direct Pay has implemented a suite of security features to encrypt and protect data from "end-to-end", complying with level 1 of the Payment Card Industry Data Security Standard. The company also proactively monitors card usage trends to detect and mitigate fraud attempts.

The privacy policy of Zoom Tanzania – a horizontal classifieds service – commits to never sharing personal details "except when required by law, or with the user's express permission". The company's business model is to encourage user-generated content and then sell advertising space through an internal network, which enables it to advertise to users without compromising their personal information.

Source: UNCTAD, 2015.

34. The main international reference frameworks used for privacy and data protection are the OECD Guidelines, the European Union Data Protection Directive and the Asia–Pacific Economic Cooperation Privacy Framework. While there is broad agreement on basic principles, there is no consensus on their application. Some data protection regimes (so-called omnibus regimes) apply equally to those processing personal data. Others apply different rules to specified sectors (for example, the health sector), types of processing entity (for example, public authorities) or categories of data (for example, data about children). In such cases, other sectors are not subject to regulatory controls.

35. A distinction can be made between regimes that operate primarily through enforcement actions brought by individuals, or their representative groups, and those that grant enforcement powers to a specialized supervisory authority that exercises ongoing oversight over the conduct of those that process personal data. An additional challenge for Governments in developing countries is the need to set up regulatory agencies.

D. Fighting cybercrime

36. Cybercrime is of growing concern to countries at all levels of development and affects both buyers and sellers. In 2012, an estimated $3.5 billion was lost in supplier revenue due to online fraud (CyberSource, 2013). In Europe, the most common forms reported by the European Consumer Centres Network were related to fraudulent websites, used cars online and counterfeit products. A common denominator among these forms is that consumers are lured by the advertisement of cheap or free products and the preferred method of payment for the fraudsters is money transfer. In developing countries, the

amount of fraud has also significantly increased. In Latin America, for example, e-commerce fraud accounts for a total of $430 million,[6] while in Africa, cybercrimes cost the Kenyan, Nigerian and South African economies an estimated $36 million, $200 million and $573 million, respectively (International Data Group Connect, 2012).

37. Such incidents highlight the challenges facing consumers online. While some crimes committed on the Internet have been around for many years, their use has expanded rapidly in terms of the number of incidents and geographically. Cybercrimes can be committed against several persons in many countries without the criminal even having to leave home. For instance, cybercriminals can route their communications through local telephone companies, long distance carriers, Internet service providers, and wireless and satellite networks, and may go through different computers located in multiple countries before attacking a particular system. Evidence may be stored on a computer in a different country from where the criminal act was executed.

38. Cybercrimes target laptops, tablets, mobile phones and entire networks. Mobile merchants are reported to be incurring the greatest fraud losses as a percentage of revenue amongst all merchant segments (LexisNexis, 2013). This represents a particular challenge for developing countries in which mobile phones are the key device for e-commerce and related payments. Moreover, developing countries are increasingly being used by cybercriminals due primarily to lax enforcement by authorities. According to one study, the top five hotspots for cybercrime are, first, the Russian Federation, followed by China, Brazil, Nigeria and Viet Nam (*Time*, 2014).

39. Cybercrime laws are rapidly being enacted. As of November 2014, 117 countries (of which 82 developing and transition economies) had enacted such legislation, and another 26 countries had draft legislation underway (UNCTAD, 2015). However, more than 30 countries had no cybercrime legislation. Africa is the region for which the largest number of countries still need to adopt cybercrime laws.

40. The most significant international instrument in the field is the Council of Europe Convention on Cybercrime (2001). It has been followed by many developing regions including through the Commonwealth Model Law on Computer and Computer-related Crime (2002) and the African Union Convention on Cyber Security and Personal Data Protection, adopted in June 2014. There are also initiatives at the European level.[7]

41. Developing countries face several issues, including a lack of capacity and infrastructure to respond effectively to cyberattacks. Cybercrime presents complicated cross-border enforcement and jurisdictional problems. Particular efforts are needed in the area of law enforcement and in strengthening the capacity of computer emergency response teams. International coordination and cooperation are critical in this context to create a safe business environment promoting faster responses and the sharing of information, thus giving countries the opportunity to react quickly and efficiently in combatting cybercrime.

[6] See http://prensa.lacnic.net/news/en/feb2014_en/study-on-cybercrime-in-the-lac-region-e-commerce-fraud-doubles (accessed 7 January 2015).

[7] See OECD (2002) and Directive 2013/40/EU of the European Parliament and of the Council of Europe of 12 August 2013 on attacks against information systems, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040&from=EN (accessed 8 January 2105).

E. Selected examples of best practices at the regional level

42. Developing regions at different levels of cyber legislation maturity have made significant advances in preparing cyberlaws through various approaches. The following examples show how the growing sophistication of cyber legislation calls for increased coordination and collaboration among regulatory/statutory authorities at national and regional levels as well as close public–private dialogue for the legislation to be successfully enacted and enforced.

43. The Association of Southeast Asian Nations, EAC and various regional groups in Latin America have all benefitted from the UNCTAD E-commerce and Law Reform Programme. Over the years, they have moved from a situation where the legal dimension of the information economy, including e-commerce legislation, was a new territory to explore, to one where the ICT dimension is being integrated into developmental policies accompanied by the necessary legal and regulatory frameworks, the latter being shaped in conformity with international standard and practices. The Programme's beneficiaries have attributed this shift to awareness-raising campaigns and to capacity-building training along with continued efforts to monitor the reform process (refer to the external evaluation by Balestrieri (2011)).

44. The Association of Southeast Asian Nations was the first developing region in 2004 to prepare a harmonized e-commerce legal framework consistent across jurisdictions. It provided guidelines to develop common objectives and principles for e-commerce legal infrastructure in support of ASEAN regional economic integration objectives through various initiatives aiming at promoting economic growth, with ICT as a key enabler for the social and economic integration of the Association. Advances have been facilitated by a joint project between AusAID and ASEAN under which regular meetings of ASEAN representatives have been organized to discuss common grounds for harmonization. Cambodia and the Lao People's Democratic Republic have been assisted by UNCTAD in the preparation of their legislation. In 2008 and in 2013, UNCTAD also reviewed the state of e-commerce harmonization in ASEAN (UNCTAD, 2013a). As part of the recommendations, further work on harmonization of cross-border jurisdiction issues was encouraged to improve cooperation among regulators and public law-enforcement agencies.

45. The harmonization of cross-jurisdiction transactions would facilitate smoother cross-border enforcement in a number of areas such as (a) recognition of electronic signatures with the mutual recognition of e-signature transactions,[8] (b) consumer protection, including an agreement between consumer protection regulators in each country, complemented by appropriate investigation and referral tools, and participation in ICPEN, which could be a first step in improving regional cooperation, and (c) cybercrime, including the establishment of a common training and resource centre and 24/7 national contact points.

46. Within EAC, partner States identified the creation of an enabling legal and regulatory environment as a critical factor for the effective implementation of e-government and e-commerce strategies at national and regional levels. Against this background and with the assistance of UNCTAD, EAC established the Task Force on Cyberlaws, composed of experts from the partner States. Since 2007, UNCTAD has been providing a mix of legal advice and training to build awareness on policy and legal issues pertaining to e-commerce. A series of consultative meetings provided an opportunity to agree on the main principles for cyberlaw harmonization and prepare two frameworks addressing various areas. An important point was to go beyond the provision of a model law and rather prepare a

[8] Some preliminary work has already been undertaken by ASEAN on this issue, including a pilot scheme between Singapore and Thailand in 2007.

baseline text to adapt to the growing sophistication of ICTs that imposes new rules and the compliance of new provisions with the existing codified normative.

47. The commitment of EAC members engaged in the reform process has been instrumental in keeping the momentum at the national level. In the case of Uganda, there was continued engagement by national authorities and private actors to contribute to the law reform process and the growing interest for ensuring its accomplishment.

48. Regional political institutions, such as the East African Legislative Assembly, stakeholder entities, such as the East African Business Council and the East African Law Society, as well as international bodies, such as UNCITRAL, UNCTAD and the Economic Commission for Africa, have been closely associated with the legal drafting and harmonization processes. In view of implementing the recommendations contained in frameworks I and II, EAC partner States have put forward a detailed list of training and awareness-raising actions for key target groups, including parliamentarians, jurists, regulatory authorities, the police and in the private sector. Great progress has been achieved.

49. In Latin America and the Caribbean, a series of 12 regional capacity-building workshops addressing over 1,100 government officials[9] has engendered multiplier effects, with a growing audience becoming acquainted with the legal aspects of e-commerce. Progress in the region has been documented in the comparative studies prepared for the region (UNCTAD, 2010b, 2010c).[10] Training offers the participants an opportunity to deepen their understanding of legal issues of e-commerce, share their experience, coordinate regional harmonization, and sensitize authorities on issues at stake at home. Human capital is essential for institutional capacity-building.

IV. Recommendations and issues for discussion

50. Buying and selling online raise legal challenges that have to be addressed by both Governments and the industry itself. Even in developed regions with a certain degree of legal harmonization, such as the European Union, different legal requirements set in national laws can hamper e-commerce. While there has been significant progress in the adoption of laws, and to some extent legal harmonization in many regions, there is still a need to align laws with leading international legal instruments to favour cross-border e-commerce. Furthermore, several Governments, especially in developing countries, need to adopt baseline laws in legal areas where they do not exist. In doing so, developing countries should coordinate among institutions tasked with different legislation on e-commerce, cloud computing and e-government to adopt common key principles that will facilitate the delivery of all these services. Governments of developing countries will also need to ensure the enforcement of laws – the next great challenge awaiting them – both domestically and across borders.

51. To support the efforts of developing countries, assistance from the regional integration communities and development partners in general should be sought to ensure compatibility of laws to foster cross-border e-commerce. Long-term capacity-building programmes should also be addressed to ensure law enforcement and ultimately the use of e-commerce.

[9] The capacity-building is organized following the TrainforTrade methodology, which provides distance-learning training facilities, an online platform where cyberlaw issues are addressed in real time by experts, and the sharing of experience among participants.

[10] An updated review will be published in 2015.

52. In close connection with these issues mentioned and focusing on regional developments, it seems relevant that experts consider the issued raised in this background document together with the processes related to e-commerce, such as those under the auspices of the World Trade Organization, OECD and the United Nations.

53. The five recommendations presented below address selected issues currently affecting e-commerce developments, with special consideration for developing countries. Participants to the meeting may wish to discuss ways to implement those recommendations and how to support coordination among regional and international institutions in the delivery of their assistance to countries in the preparation and enforcement of their cyberlaws.

54. **Aligning laws for e-transactions:** Ensuring regional and global harmonization of e-transactions is a key challenge of the increased use of electronic technologies by Governments, companies and citizens. When preparing or revising e-commerce legislation, lawmakers should consider that of other countries in the same region or of trading partners in order to have compatible legal systems and trade policies. It is important to consider the legal recognition of e-signatures, electronic contracts and evidence not only at a national level but also when originating from other jurisdictions.

55. Over the past 10 years, advances towards harmonization have been made in several regions. However, as different standards are used, there is still a need to make laws more compatible internationally. The United Nations Convention on the Use of Electronic Communications in International Contracts can help in promoting legal harmonization. It proposes a set of core legal provisions enabling cross-border e-commerce. Countries should consider aligning their legislation on e-transactions with the provisions of this Convention. Becoming a party to it will favour regional and international harmonization, including the cross-border recognition of e-signatures as the Convention provides principles that could form the basis of a mutual recognition system. The Convention updates certain provisions of UNCITRAL model laws, such as the location of the parties; the time and place of dispatch and receipt; and the functional equivalence of "signature". It also introduces new provisions such as the use of automated message systems, invitation to make offers, and the like. Finally, the Convention provides core provisions on e-transactions to ensure regional and international harmonization. Some countries have already modified their domestic legislation in line with the substantive provisions of the Convention.

56. **Streamlining consumer protection policies:** Differences in national consumer protection laws are a challenge for cross-border e-commerce. Efforts at harmonizing consumer protection laws in e-commerce are carried out by various regional groupings.

57. Countries that are preparing or revising their consumer protection laws for e-commerce may consider aligning their legislation with the United Nations Guidelines on Consumer Protection and the OECD Guidelines to encourage harmonization of consumer protection legislation and foster consumer confidence in e-commerce.

58. There is a need to set up consumer protection agencies in several developing countries and to strengthen existing ones in other countries. In addition, the implementation of regional mechanisms for online consumer complaints and enforcement would facilitate cross-border e-commerce. This would require an agreement between consumer protection agencies in a given region, complemented by appropriate investigation and referral tools. Linking up agencies through networks such as ICPEN can help national agencies to keep abreast of new legal regional or international developments, as well as to share experiences and bring out solutions for e-commerce users.

59. The use of alternative dispute resolution and redress schemes that are affordable and easy to use is also recommended. Some of the most effective schemes are currently embedded in self-regulatory bodies, law enforcement agencies, ombudsmen and other

entities. The use of trustmarks, such as the eConfianza[11] initiative of the E-Commerce Latin American Institute (eInstituto), is furthermore worth exploring. A non-profit organization, eInstituto has created a code of good practices to guide companies on how to address consumer needs properly when designing their online businesses. It also offers an online dispute-resolution tool called Pactanda.[12]

60. **Streamlining data protection and cybercrime laws:** The development and adoption of legal frameworks for protecting personal data and for combating cybercrime at the national level to ensure confidence and trust in the use of the Internet should not be done in isolation. Harmonization of laws and policies is required at the regional and international levels. The establishment of minimum standards helps to ensure cross-border coordination on the design and implementation of relevant legislation and stronger enforcement institutions.

61. Establishing an efficient data protection regulatory agency can be challenging from both a resource and a political perspective. Lessons may be learned from the telecommunications sector, where such agencies have been widely accepted as a critical component of a successful regulatory regime. Combining regulatory functions between data protection and consumer protection agencies may be a way to reduce the regulatory costs of data protection.

62. Similarly, comprehensive frameworks for cooperation outreach and enforcement of cybercrime need to be developed. Investigating even a single communication may require cooperation among the law enforcement agencies of several countries (including the private sector) as law enforcement is typically restricted by national borders. Regional cooperation between cybercrime law enforcement agencies may involve the establishment of a common training and resource centre and 24/7 national contact points.

63. Various security measures – physical, logical or organizational – should be used to protect data against deliberate acts of misuse. Implementing appropriate data security should consider the quality of data, the needs of individual data subjects, the entity processing the personal data and, indeed, society at large. Policymakers are increasingly recognizing the Internet as a "critical national infrastructure", on which a rising proportion of economic and social activities relies, but also as a "source of vulnerability". Addressing this duality and putting in place adequate data security measures, from the adoption of cybercrime laws to the establishment of computor emergency response teams/computer security incident response teams, should be a core component of the policy response. Furthermore, public–private partnerships should be implemented to take advantage of private sector strengths and responses to ICT threats.

64. **Strengthening the capacity of lawmakers and the judiciary:** The judiciaries in many developing countries need to be trained in the area of cyberlaws. Legal issues around e-commerce are still relatively new. Several international and regional organizations, including the Commonwealth secretariat, the International Telecommunication Union, UNCITRAL, UNCTAD, the United Nations Office on Drugs and Crime and the Council of Europe can provide assistance to countries and regions in the different legal areas. Increasingly, these agencies are joining forces to maximize their actions (box 2).

[11] See www.econfianza.org (accessed 9 January 2015).

[12] Available at www.pactanda.com (accessed 9 January 2015).

Box 2. Assistance provided by UNCTAD and partners

In support of developing countries' efforts in this area, UNCTAD assists in the preparation and revision of e-commerce laws aligned with international and regional instruments. The assistance provided in the harmonization of e-commerce legislation across regions in ASEAN, EAC, ECOWAS, Latin America and Central America has created an impetus for countries to push for adopting national laws in this area. The work has involved close collaboration with regional institutions such as the African Union Commission, the ASEAN secretariat, the EAC secretariat, the ECOWAS Commission, the Asociación Latinoamericana de Integración and the Sistema Económico Latinoamericano y del Caribe.

Capacity-building activities have strengthened the knowledge of policymakers and lawmakers on legal issues of e-commerce and international best practice, allowing them to formulate laws in line with their regional frameworks.

Several agencies are assisting developing countries within the scope of their mandates, and inter-agency collaboration is growing. Two examples of such cooperation are the briefing of Commonwealth parliamentarians, serviced by UNCTAD and organized jointly with the Commonwealth Telecommunication Organization and the Commonwealth Parliamentary Association, at the occasion of the Commonwealth Cybersecurity Forum 2013. Another example is the joint workshop on the harmonization of cyber legislation in ECOWAS (Ghana, March 2014) organized by UNCTAD with UNCITRAL, the African Centre for Cyberlaw and Cybercrime Prevention, the Council of Europe, and the Commonwealth Cybercrime Initiative.

UNCTAD has built a network of institutions with which consolidated partnerships are concluded within the different project activities. Many of the partners have contributed to the consolidation of the database used in this chapter. The result of this first-ever global mapping is available online and countries are invited and encouraged to contribute to keeping this database up-to-date.

Source: UNCTAD.

65. **Enhancing the awareness of consumers and companies:** As the legal environment for e-commerce is evolving, and differs from one jurisdiction to another, consumers and enterprises need to be aware of relevant laws and means of redress. This is particularly important to build trust in cross-border e-commerce. Industry associations and consumer protection agencies should work together to overcome barriers caused by divergent national legal standards. National public campaigns (including through radios and television programmes) to inform about ways to protect consumers online can be a key element of awareness-raising strategies.

Box 3. Awareness-raising activities in Uganda

In Uganda, the National Information Technology Authority and the Ministry of Information and Communications Technology have developed and enacted subsidiary legislation (the Electronic Transactions Act and Electronic Signatures Act) to operationalize the EAC Framework on Cyber Laws (UNCTAD, 2012). Since 2011, the National Information Technology Authority has embarked on raising awareness about these laws as well as aspects of information security to encourage public administration and the private sector to put in place minimum information security controls to ensure safe e-transactions. Several sensitization workshops were organized for entities such as ministries, banker associations, law societies, national chambers of commerce, the Investment Authority and the Securities Exchange. Workshops have been facilitated by a multi-institutional team of lawyers and technical resource persons, including experts participating in the EAC Task Force on Cyberlaws supported by UNCTAD. Future plans include the delivery of similar workshops to create awareness on the Data Protection and Privacy Bill, once enacted.

Source: UNCTAD.

66. Against this background, experts are invited to consider the following questions related to the current salient legal challenges facing countries for e-commerce development at both domestic and cross-border levels:

- How can the needs of countries in terms of cyberlaws best be assessed?
- What are best practices to foster cross-border transactions and improve security of e-transactions?
- What role should the private sector play in securing transactions online and fostering consumer trust and confidence?
- What actions should be taken to monitor the progress of developing countries and regions in developing relevant cyber legislation?
- How can assistance from international organizations and development partners help to facilitate the enforcement of compatible e-commerce laws?

References

Balestrieri E (2011). External evaluation of UNCTAD's E-Commerce and Law Reform Project. Available at http://tft.unctad.org/wp-content/uploads/2014/03/2011Evaluation.ICT_.law_.Report.pdf (accessed 9 January 2015).

Castellani L (2010). The United Nations electronic communications convention: Policy goals and potential benefits. *Korean Journal of International Trade and Business Law*. 19(1):1–16.

CyberSource (2013). 2013 online fraud report. Available at http://www.cybersource.com/resources/collateral/Resource_Center/whitepapers_and_reports/CyberSource_2013_Online_Fraud_Report.pdf (accessed 9 January 2015).

European Commission (2011). Consumer attitudes towards cross-border trade and consumer protection. Eurobarometer No. 299. European Commission. Brussels.

Innopay (2012). Online payments 2012 – Moving beyond the web. Innopay B.V. Amsterdam. Available at http://www.innopay.com/publications/online-payments-2012-moving-beyond-web (accessed 9 January 2015).

International Data Group Connect (2012). Africa 2013: Cyber-crime, hacking and malware. White paper available from www.idgconnect.com/view_abstract/11401/africa-2013-cyber-crime-hacking-malware (accessed 8 January 2015).

LexisNexis (2013). True cost of fraud 2013 study: Manage retail fraud. Available at http://www.lexisnexis.com/risk/insights/2013-true-cost-fraud.aspx (accessed 9 January 2015).

OECD (2000). *Guidelines for Consumer Protection in the Context of Electronic Commerce*. OECD. Paris.

OECD (2002). *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. OECD. Paris.

OECD (n/d). Recommendation of the OECD council concerning guidelines for consumer protection in the context of electronic commerce. OECD. Paris. Available at http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=183&InstrumentPID=179&Lang=en&Book= (accessed 13 January 2015).

Risk Based Security (2014). Data breach quickview: An executive's guide to 2013 data breach trends. Available at https://www.riskbasedsecurity.com/reports/2013-DataBreachQuickView.pdf (accessed 9 January 2015).

Time (2014). The world's top 5 cybercrime hotspots. 7 August. Available at http://time.com/3087768/the-worlds-5-cybercrime-hotspots/ (accessed 12 January 2015).

UNCITRAL (1999). *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5* bis *as adopted in 1998*. United Nations publication. Sales No. E.99.V.4. New York.

UNCITRAL (2002). *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001*. United Nations publication. Sales No. E.02.V.8. New York.

UNCITRAL (2007). *United Nations Convention on the Use of Electronic Communications in International Contracts*. United Nations publication. Sales No. E.07.V.2. New York.

UNCTAD (2001). United Nations Guidelines for Consumer Protection (as expanded in 1999). UNCTAD/DITC/CLP/Misc.21. New York and Geneva. Available at http://unctad.org/en/Docs/poditcclpm21.en.pdf (accessed 13 January 2015).

UNCTAD (2010a). *Information Economy Report 2010: ICTs, Enterprises and Poverty Alleviation*. United Nations publication. Sales No. E.10.II.D.17. New York and Geneva.

UNCTAD (2010b). *Estudio Sobre Las Perspectivas de La Armonización de La Ciberlegislación En Centroamérica Y El Caribe*. United Nations publication. UNCTAD/DTL/STICT/2009/3. New York and Geneva.

UNCTAD (2010c). *Study on Prospects for Harmonizing Cyberlegislation in Latin America*. United Nations publication. UNCTAD/DTL/STICT/2009/1. New York and Geneva.

UNCTAD (2012). *Harmonizing Cyberlaws and Regulations: The Experience of the East African Community*. United Nations publication. UNCTAD/DTL/STICT/2012/4. New York and Geneva.

UNCTAD (2013a). *Review of E-commerce Legislation Harmonization in the Association of Southeast Asian Nations.* United Nations publication. UNCTAD/DTL/STICT/2013/1. New York and Geneva.

UNCTAD (2013b). *Information Economy Report 2013: The Cloud Economy and Developing Countries*. United Nations publication. Sales No. E.13.II.D.6. New York and Geneva.

UNCTAD (2015). *Information Economy Report 2015: Unlocking the Potential of E-Commerce for Developing Countries*. United Nations publication. New York and Geneva (forthcoming).

WorldPay (2014). Alternative payments report, 2nd edition. Available at http://www.worldpay.com/global/alternative-payments-2nd-edition (accessed 12 January 2015).