United Nations A/CN.9/657/Add.1

General Assembly

Distr.: General
2 June 2008

Original: English

[Start1]

United Nations Commission on International Trade Law
Forty-first session
New York, 16 June-3 July 2008

Current activities of international organizations related to the harmonization and unification of international trade law

Note by the Secretariat

Contents

	Paragraphs	Page
F. Security Interests	1-14	2
G. Electronic commerce and new technologies	15-53	5

V.08-54043 (E) 090608 100608

F. Security Interests

General

1. Coordination meetings were held in September 2007 in Rome and in May 2008 in New York among the secretariats of the Hague Conference on Private International Law, the International Institute for the Unification of Private Law (Unidroit) and UNCITRAL. The main topic discussed at these meetings was the interrelationship among the texts on security interests prepared by the Hague Conference, Unidroit and UNCITRAL, and ways in which States could adopt these texts to establish a modern comprehensive and consistent legislative regime on secured transactions.

2. Further to those meetings, the three organizations have recognized that policymakers in States may have difficulty determining how their various instruments with respect to security interests fit together, which ones would best serve the policy goals of the State and whether implementing one instrument precludes the implementation of another. Thus, the three organizations are preparing a paper aimed at assisting policymakers by summarizing the scope and application of those instruments, showing how they work together, noting which of them would serve the policy goals of the State and providing a comparative understanding of the coverage and basic themes of each instrument. The paper will be prepared in a manner that is easily understood by non-experts in secured transactions, and it will be made available to States to assist them in considering the implementation of the instruments.

Unidroit[1]

(a) Draft convention on substantive rules regarding intermediated securities

3. Coordination continued to ensure consistency between the draft convention on substantive rules regarding intermediated securities and the UNCITRAL Legislative Guide on Secured Transactions. In order to avoid any overlap and conflict, the Commission decided that all securities should be excluded from the scope of the Guide (see A/62/17 (Part I), paras. 147 and 160). The Commission also decided that future work should be undertaken on certain types of securities not covered by the draft Convention and the Guide. The Commission also decided that payment rights arising from or under financial contracts governed by netting agreements, as well as from or under foreign exchange transactions, should also be excluded from the scope of the Guide, and that future work on financial contracts should be considered at a future session (ibid. paras. 147 and 161).

(b) Preliminary draft model law on leasing

4. The Unidroit Committee of governmental experts preparing a preliminary draft Model Law on leasing, at its meetings in Johannesburg, South Africa in May 2007 and in Muscat, Oman in April 2008, approved the joint proposal of the secretariats of Unidroit and UNCITRAL to exclude from the preliminary draft model law "a leasing agreement that creates a security right or an acquisition security right, as defined in the UNCITRAL Legislative Guide on Secured

[1] www.unidroit.org.

Transactions" (see article 3, paragraph 1 of the preliminary draft model law). At its meeting in April 2008 in Rome, the Governing Council of Unidroit approved the preliminary draft model law, subject to some minor translation adjustments, and authorized the Unidroit secretariat to transmit the draft model law to Governments for finalization and adoption at a joint session of the Unidroit General Assembly, meeting in extraordinary session, and the Unidroit Committee of Governmental Experts, to be held in Rome later in 2008.

(c) Protocols to the Convention on International Interests in Mobile Equipment (Cape Town Convention)

5. Both the Convention and the Protocol thereto on Matters specific to Aircraft Equipment, opened for signature in Cape Town on 16 November 2001, continue to attract new Contracting States. For an up-to-date picture of the situation in this regard, the reader is directed to the Unidroit website (www.unidroit.org).

6. The Protocol to the Convention on Matters specific to Railway Rolling Stock, opened for signature in Luxembourg on 23 February 2007, currently has four signatory States. The Preparatory Commission established at the diplomatic Conference in Luxembourg to act as Provisional Supervisory Authority of the International Registry for railway rolling stock pending entry into force of the Protocol, at its second session, held in Rome from 8 to 10 April 2008, appointed CHAMP, a company based in Luxembourg, as Registrar of the future International Registry for railway rolling stock.

Preliminary draft Protocol to the Convention on Matters specific to Space Assets

7. Following the intersessional work accomplished by two joint Government/industry meetings called by Unidroit and the Space Working Group to consider the work accomplished by the Secretariat in pursuance of the assignments handed out by the Unidroit Committee of governmental experts at its second session, held in Rome from 26 to 28 October 2004, the Unidroit General Assembly at its 61st session, held in Rome on 29 November 2007, endorsed the Secretariat's proposal for the establishment of a Steering Committee, open to the Governments and the representatives of the international commercial space and financial communities that had participated in the aforementioned Government/industry meetings, to build consensus around the provisional conclusions reached at the second of those meetings, notably a narrowing of the sphere of application of the preliminary draft Protocol so as to concentrate essentially on the satellite, in its entirety. The Steering Committee held its launch meeting in Berlin from 7 to 9 May 2008. On that occasion it agreed on the steps necessary to permit an early resumption of the intergovernmental consultation process and finalization of the proposed Protocol.

Possible future Protocol to the Convention on Matters specific to Agricultural, Construction and Mining Equipment

8. At its 87th session, the Unidroit Governing Council authorized the Secretariat to continue its research into the possible preparation of an additional Protocol on Matters specific to Agricultural, Construction and Mining Equipment.

European Commission[2]

(a) Rome I regulation

9. The European Commission adopted a regulation on the law applicable to contractual obligations (Rome I). Article 14 deals with the law applicable to the relationship between an assignor and an assignee under a voluntary assignment or contractual subrogation of a claim and the relationship between the assignee and the debtor in a way that is consistent with the United Nations Convention on the Assignment of Receivables in International Trade ("the United Nations Assignment Convention"). The European Commission was asked to study the matter of the law applicable to third-party effects of assignments, a matter also addressed in the United Nations Assignment Convention. The UNCITRAL secretariat will continue its dialogue with the European Commission with a view to avoiding conflicts between the Convention and any future European Commission instrument on the matter.

(b) The UNCITRAL Legislative Guide on Secured Transactions

10. The European Commission submitted to the Commission comments on the draft Legislative Guide on Secured Transactions (A/CN.9/633). In order to address the comments, the Commission, at its fortieth session, decided to: (a) exclude all securities payment rights arising from or under financial contracts and foreign exchange transactions; (b) undertake work on security interests in intellectual property; (c) offer an expanded non-unitary approach to acquisition financing; (d) review its conflict-of-laws provisions (see A/62/17 (Part I) paras. 158-162). With regard to the last topic, at its resumed fortieth session, the Commission confirmed the approach followed in the United Nations Assignment Convention with regard to the law applicable to third-party effects of assignments, but agreed to explain further in the commentary the alternative approach based on the law governing the assigned receivable (see A/62/17 (Part II) paras. 82-92).

WIPO[3]

11. Coordination with WIPO experts continued with respect to the preparation of the working paper discussed by Working Group VI at its thirteenth session held in New York in May 2008 (A/CN.9/WG.VI/WP.33 and Add.1, see A/CN.9/649 for the outcome of those discussions).

The Hague Conference[4]

12. The work of the Hague Conference on security interests in the past year was focused on post-Convention activities in respect of the 2006 Hague Convention on the Law Applicable to Certain Rights in Respect of Securities (Hague Securities Convention). In particular, the Permanent Bureau continued its efforts to disseminate and provide assistance with respect to the Securities Convention. An interesting development in that regard was reported to be the signature of this Convention by Mauritius, a rapidly growing financial centre for the Pacific region,

---

[2] ec.europa.eu.

[3] www.wipo.int.

[4] www.hcch.net.

which had been undergoing a major revision and modernization of its financial legislation. Furthermore, the Hague Conference pursued its continuing efforts to promote the 1985 Trusts Convention, which includes the creation of trusts for security purposes. This Convention entered into force for Switzerland on 1 July 2007 and was acceded to on 1 June 2007 by Monaco, where the Convention shall enter into force on 1 November 2008.

13. In addition, the Permanent Bureau of the Hague Conference was also involved in the preparation of an annex to the UNCITRAL Legislative Guide on Security Transactions on security rights relating to intellectual property rights (see A/CN.9/649).

OAS[5]

14. The Organization of American States adopted a Model Inter-American Law on Secured Transactions in February 2002 at its sixth Inter-American Specialized Conference on Private International Law (CIDIP-VI). During preparations for CIDIP-VII, Member States have undertaken potential instruments for secured transactions registries needed to complement the Model Law. These instruments include the following: (1) Uniform Inter-American Registration Forms, including Amendment Form, Continuation Form, Cancellation Form, and Enforcement Form; (2) Model Rules for Secured Transactions Registries, including guidelines for both filing process and registry operation; and (3) Model Rules for Electronic Registries, including electronic signatures, certification, and multinational registry interconnectivity. In 2008, the OAS General Assembly urged Member States to present working documents on all three instruments. As a result, the delegations of the United States, Canada and Mexico formed an informal committee to prepare preliminary drafts of each. Once presented, the formal working group, also reconvened by the General Assembly in 2008 with governmental and independent experts, will complete the preparatory work, prior to convening a final diplomatic conference.

G. Electronic commerce and new technologies

General

15. The UNCITRAL Model Law on Electronic Commerce,[6] the UNCITRAL Model Law on Electronic Signatures,[7] as well as the Convention on the Use of Electronic Communications in International Contracts,[8] provide a good basis for States to facilitate electronic commerce, but only address a limited number of issues. More steps are required to enhance confidence and trust in electronic commerce. They include: appropriate rules on consumer and privacy protection, cross-border recognition of electronic signatures and authentication methods,

---

[5] www.oas.org.

[6] For the text of the Model Law, see *Official Records of the General Assembly, Fifty-first Session, Supplement No. 17* (A/51/17), annex I.

[7] For the text of the Model Law, see *Official Records of the General Assembly, Fifty-sixth Session, Supplement No. 17* (A/56/17), annex II.

[8] For the text of the Convention, see the Annex to General Assembly resolution 60/21, of 23 November 2005.

measures to combat computer crime and cybercrime, network security and critical infrastructure for electronic commerce and protection of intellectual property rights in connection with electronic commerce, among various other aspects.

16. A number of organizations are currently working on various aspects related to the matters referred to above. To a large extent, this work is of a technical nature or is essentially aimed at capacity-building. Some initiatives, however, have taken the form of policy or legislative guidance, and the Commission may wish to take note of them. Those more directly relevant for the Commission's work on electronic commerce are summarized below.

ITU[9]

17. The International Telecommunications Union (ITU) is currently working on a Toolkit for Cybercrime Legislation.[10] The document ITU-D Study Group Q22/1 had already identified measures aimed at deterring cybercrime as integral components of a national cybersecurity/CIIP strategy. ITU advocates, in particular, the adoption of appropriate legislation to combat the misuse of information and communication technology (ICT) for criminal or other purposes and to prevent activities intended to affect the integrity of national critical infrastructures. As threats can originate anywhere around the globe, the challenges are inherently international in scope and it is desirable to promote harmonization towards international best practices in combating cybercrime.

18. The Toolkit for Cybercrime Legislation aims to provide countries with reference material that can assist in the establishment of a legislative framework to deter cybercrime. Development of the toolkit is by a multidisciplinary international group of experts and a first draft was anticipated in the first quarter of 2008.

19. Cybercrime is not an area directly related to the field of work of UNCITRAL. Nevertheless, to the extent that cybercrime negatively affects international trade, it becomes a matter of concern from the Commission's perspective. Use of modern information and communication technologies has provided new means for criminal, fraudulent or indecent activities, such as embezzlement of funds, slander, and industrial espionage, violation of trade secrets or dissemination of child pornography. At the same time, new types of criminal conduct have emerged, such as identity theft, dissemination of computer viruses, or intentional breakdown of computer and information services. Besides their criminal character, all these activities may significantly affect international trade by causing physical loss or moral damage to individuals and business entities and by undermining business and consumer confidence in electronic commerce.

20. The Commission way wish to take note of the work being done by ITU, which does not directly affect the area of work of UNCITRAL, but which is, by establishing an effective legal framework for preventing and prosecuting computer crime and cybercrime, an essential component of domestic and international strategies to promote electronic commerce.

---

[9] www.itu.int.

[10] http://www.itu.int/ITUD/cyb/cybersecurity/projects/cyberlaw.html.

APEC[11]

21. The Asia-Pacific Economic Cooperation (APEC) has also been active in the area of cybercrime and security.[12] The APEC Cyber-Security Strategy, for instance, includes a package of measures to protect business and consumers from cybercrime, and to strengthen consumer trust in the use of e-commerce. One notable initiative is the development of key public infrastructure guidelines to facilitate cross-jurisdictional e-commerce.

22. A number of countries in the APEC region are currently implementing and enacting cyber-security laws, consistent with the General Assembly resolution 55/63, of 4 December 2000, and the Convention on Cybercrime adopted by the Council of Europe (Budapest, 23 November 2001)[13] and its Protocol.[14] Against that background, the APEC Telecommunications and Information Working Group (TEL) has launched a Cyber-crime Legislation Initiative and Enforcement Capacity Building Project which is aimed at supporting domestic institutions of APEC member countries to implement new laws.

23. APEC has developed guidelines for establishing and operating so-called Computer Emergency Response Teams (CERTs) as early warning defence systems against cyber attacks. APEC is providing training to domestic officials of APEC countries in connection with the implementation of CERTs. The protection of small and medium-sized enterprises is a priority under the APEC Cyber Security Strategy. Practical tools for protecting small businesses from attacks and spreading viruses have been developed, including advice on how to use the internet securely, safety issues relating to wireless technologies and safe e-mail exchanges.

24. It is expected that work on reducing the criminal misuse of information will continue to be a priority for TEL and will focus on the importance of sharing information; developing procedures and mutual assistance laws, and other measures to protect business and citizens.

25. The Commission way wish to take note of the work being done by APEC, which, like similar work being done by ITU, does not directly affect the area of work of UNCITRAL, but which is, by establishing an effective legal framework for preventing and prosecuting computer crime and cybercrime, an essential component of domestic and international strategies to promote electronic commerce.

---

[11] www.apec.org

[12] http://www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.htm.

[13] The CyberCrime Convention, ETS 185, entered into force on 1 July 2004. It is intended to develop a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate criminal legislation and fostering international cooperation. *Source*: Council of Europe Treaty Office, http://conventions.coe.int/.

[14] The Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Acts of a Racist and Xenophobic Nature supplements, as between the Parties to the Protocol, the provisions of the Convention on Cybercrime as regards the criminalization of acts of a racist and xenophobic nature committed through computer systems (ETS 189). It was opened for signature in Strasbourg on 28 January 2003. Source: Council of Europe Treaty Office, http://conventions.coe.int.

OECD[15]

26. The Organization on Economic Cooperation and Development (OECD) is currently working on various aspects of the use of information and communication technologies that are relevant for the electronic commerce from the perspective of UNCITRAL. The main aspects of this work are summarized below.[16]

Electronic Authentication

27. On 12 June 2007, the OECD Council adopted its Recommendation on Electronic Authentication and Guidance for Electronic authentication. The Recommendation encourages efforts by OECD member States to establish compatible, technology-neutral approaches for effective domestic and cross-border electronic authentication of persons and entities. The full text of the Recommendation is available on the OECD website.

28. The OECD has also developed a guidance document on electronic authentication to assist Member countries and non-Member economies in establishing or amending their approaches to electronic authentication with a view to facilitating cross-border authentication. The Guidance sets out the context and importance of electronic authentication for electronic commerce, electronic government and many other social interactions. It provides a number of foundation and operational principles that constitute a common denominator for cross-jurisdictional interoperability.

29. Both the Recommendation and the Guidance conclude a work-stream initiated in response to the "Declaration on Authentication for Electronic Commerce" adopted by Ministers at the Ottawa Ministerial Conference held on 7-9 October 1998 and serve as a bridge to future OECD work on identity management.

30. This line of work by OECD is directly relevant to the Commission's work on electronic commerce. Article 12 of the UNCITRAL Model Law on Electronic Signatures, for example, encourages States to promote cross-border recognition of electronic signatures. Paragraph 1 of that article reflects the basic principle that the determination of whether and to what extent a certificate or an electronic signature is capable of being legally effective should not depend on the place where the certificate or the electronic signature was issued but on its technical reliability. Paragraph 2 of that article provides the general criterion for the cross-border recognition of certificates without which suppliers of certification services might face the unreasonable burden of having to obtain licenses in multiple jurisdictions. The threshold for technical equivalence of foreign certificates is based on testing their reliability against the reliability requirements established by the enacting State pursuant to the Model Law, regardless of the nature of the certification scheme obtaining in the jurisdiction from which the certificate or signature originates.

31. Article 12, paragraphs 2 and 3, of the Model Law on Electronic Signatures deal exclusively with the cross-border reliability test to be applied when assessing the reliability of a foreign certificate or electronic signature. However, in the preparation of the Model Law, it was borne in mind that enacting States might wish to obviate the need for a reliability test in respect of specific signatures or

[15] www.oecd.org.

[16] http://www.oecd.org/findDocument/0,3354,en_2649_37441_1_119820_1_1_37441,00.html.

certificates, when the enacting State was satisfied that the law of the jurisdiction from which the signature or the certificate originated provided an adequate standard of reliability. As to the legal techniques through which advance recognition of the reliability of certificates and signatures complying with the law of a foreign country might be made by an enacting State (e.g. a unilateral declaration or a treaty), the Model Law contains no specific suggestion.

32. The lack of common standards for cross-border recognition of electronic signatures and other authentication methods is considered to be a significant impediment to cross-border commercial transactions. Two main problems exist in the given context. On the one hand, technological measures and systems for electronic signatures, in particular digital signatures, are currently much too diverse to enable uniform international standards. On the other hand, fears about fraud and manipulation in electronic communications have led some jurisdictions to establish rather stringent regulatory requirements, which in turn may have discouraged the use of electronic signatures, in particular digital signatures.

33. Wide accession of the recently adopted United Nations Convention on the Use of Electronic Communications in International Contracts, which provides in its article 9 for the functional equivalence between electronic signatures and traditional types of signature, may go a long way towards facilitating cross-border use of electronic signatures. Nevertheless, notarization of electronic documents and electronic signatures in government or other official records are areas in which governments may be inclined to retain national standards capable of hindering or barring recognition of foreign electronic signatures.

34. Although the OECD recommendations and guidance are not primarily concerned with legal matters, they make reference to the principles of legal recognition of electronic signatures and technology neutrality, which are two of the basic principles of the UNCITRAL Model Law on Electronic Signatures:

> "The use of electronic signatures for producing legal effect equivalent to handwritten signatures raises several issues which are addressed by the UNCITRAL 2001 Model Law on Electronic Signatures. OECD Member countries support the use of electronic signatures as equivalent to handwritten signatures and advocate technology neutrality in their use."[17]

35. The essential element of the OECD recommendations and guidance will be reflected in the final version of the publication on authentication and cross-border recognition of electronic signatures, which the Secretariat plans to issue later this year, following the Commission's request at its fortieth session.[18] The Commission may wish to take note of the work being done by OECD in this area in light of its previous affirmation that technology neutrality, cross-border recognition and technical interoperability are three essential components of a favourable policy framework to facilitate the use of electronic signatures and authentication methods in international trade.

---

[17] http://www.oecd.org/dataoecd/32/45/38921342.pdf.

[18] *Official Records of the General Assembly, Sixty-second Session, Supplement No. 17* (A/62/17), para. 195.

Consumer Dispute Resolution and Redress

36. Another area related to electronic commerce in which OECD has been working concerns consumer protection. On 12 July 2007, OECD adopted a Recommendation on Consumer Dispute Resolution and Redress aimed at providing governments with a framework to help consumers resolve disputes and settle claims with business.[19] Again, the full text of the recommendation is available on the OECD's website.

37. The annex to the recommendation covers disputes in both domestic and cross-border transactions. The recommendation was developed to deal with issues arising from the rapid growth in electronic commerce, but it will also benefit consumers making traditional types of purchases. The Chairman of the OECD Committee on Consumer Policy (CCP), which prepared the recommendation, explains its rationale as follows:

> "E-commerce has allowed consumers access to an expanding range of goods and services. Recent studies [however] have shown that consumers may be reluctant to take full advantage of shopping on-line because of concerns about dispute resolution if they are unsatisfied with their purchase. The Recommendation provides a practical approach to address these concerns in a systematic and comprehensive way."[20]

38. The recommendation aims at addressing the current practical and legal obstacles to pursuing remedies in consumer cases, whether locally or cross-border contexts. The annex to the recommendation focuses on five priority areas for attention: identifying basic elements needed for effective domestic resolution and redress frameworks; improving resolution of cross-border disputes; enhancing the scope and effectiveness of private sector initiatives to resolve disputes; developing information for monitoring developments and trends in consumer complaints; and improving consumer and business education and awareness on ways to avoid and handle disputes.

39. The domestic framework described in the annex to the recommendation calls on governments to provide consumers with mechanisms allowing them to act individually, such as alternative dispute resolution services and simplified procedures for small claims courts, or collectively, such as actions initiated by a consumer in his name and representing other consumers. It also covers actions initiated by consumer organizations representing consumers, actions initiated by consumer protection enforcement authorities acting as representative parties for consumers. Consumer protection enforcement authorities may obtain or facilitate redress on behalf of consumers, allowing them to seek court orders in civil and criminal proceedings and to act as a representative party in lawsuits seeking redress. In the context of cross-border disputes, the recommendation calls on Member countries to improve awareness of, and access to, dispute resolution and redress mechanisms and to enhance the effectiveness of remedies.

40. UNCITRAL has consistently refrained from dealing with matters related to consumer protection. Article 2, subparagraph 1 (a) of the Convention on the Use of Electronic Communications in International Contracts, for example, clearly

---

[19] http://www.oecd.org/dataoecd/43/50/38960101.pdf.

[20] http://www.oecd.org/document/53/0,3343,en_2649_34267_38960053_1_1_1_1,00.html.

excludes consumer transactions from its scope. Most electronic commerce nowadays is done between business entities. However, the share of consumer transactions is increasing and in some industries is the prevailing market. Lack of appropriate rules, guidelines or voluntary codes of conduct for consumer protection in an electronic environment, or even the perception of insufficient legal protection, undermine confidence in electronic commerce and constitute an obstacle to its development. Conflicting standards across borders may also affect the offer of goods and services, as business entities operating under a less developed or excessively tolerant framework may enjoy an unfair competitive advantage, as compared to companies required to comply with more stringent requirements. In some cases, operations under a more lenient legal framework may be favoured by business entities interested in shielding themselves from liability that may arise under more stringent regimes. The interest of attracting investment by these companies may need to be weighed against the risk that the host country might be perceived as a safe harbour for unfair business practices, which may damage the reputation of an entire business sector.

41. The work being done by the OECD in this area is also relevant for UNCITRAL from the point of view of its past and ongoing work in the area of commercial dispute resolution. Online dispute resolution in a business context is indeed one of the items which the Commission requested Working Group I (International arbitration and conciliation) to place on its agenda but and consider, at least in an initial phase, in the context of the revision of the UNCITRAL Arbitration Rules.[21]

Cross-border Co-operation in the Enforcement of Laws Protecting Privacy

42. Privacy protection has been on the agenda of OECD for a long time and has led the organization to formulate well-known instruments. The latest instrument is the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, which was adopted by the OECD Council on 12 June 2007.[22] The full text of the recommendation is available on the website of the OECD.

43. The recommendation was developed by the OECD Committee for Information, Computer and Communications Policy (ICCP), through its Working Party on Information Security and Privacy (WPISP). The recommendation is grounded in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980).[23] It was adopted to provide a new framework for cooperation in the enforcement of privacy laws. The recommendation was motivated by recognition that changes in the character and volume of cross-border data flows have elevated privacy risks for individuals and highlighted the need for better cooperation among the authorities charged with providing them protection.

---

[21] *Official Records of the General Assembly, Sixty-first Session, Supplement No. 17* (A/61/17), para. 187.

[22] http://www.oecd.org/dataoecd/43/28/38770483.pdf.

[23] See OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, applicable on 23 September 1980, http://www.oecd.org/document/18/0,2340, en_2649_34255_1815186_1_1_1_1,00.html. See further the OECD "Privacy Policy Generator" (http://www.oecd.org/document/39/0,2340,en_2649_34255_28863271_1_1_1_1,00.html).

44. The framework contained in the annex to the recommendation, and which is embodied therein by reference, reflects a commitment by OECD governments to improve their domestic frameworks for privacy law enforcement to better enable their authorities to cooperate with foreign authorities, as well as to provide mutual assistance to one another in the enforcement of privacy laws. The OECD has developed two model forms to facilitate privacy law enforcement cooperation. The first is a form to assist in the creation of a list of contact points in each country to coordinate requests for assistance. The second is a form for use by an authority in requesting assistance to help ensure that key items of information are included in the request.

45. Lack of confidence in the privacy and security of online transactions and information networks is seen as an element possibly preventing economies from gaining all of the benefits of electronic commerce. On the other hand, regulatory systems restricting the flow of information can have adverse implications for global business and economies. New issues and restrictions on data protection arise from international security concerns, which have led to legislative actions directed at data retention. With a growing stock of international rules these do not only become more heterogeneous but also make it more difficult for companies to comply. As these standards consider conflicting interests the delineation of the field of application of these instruments as well as which of the interests protected will prevail in a specific case is gaining growing importance.

46. Concerns over privacy protection may affect domestic and international electronic commerce in many ways. Conflicting standards across borders may also affect the offer of goods and services, as business entities operating under a less developed or excessively tolerant framework may enjoy an unfair competitive advantage, as compared to companies required to comply with more stringent requirements. In some cases, operations under a more lenient legal framework may be favoured by business entities interested in shielding themselves from liability that may arise under more stringent regimes. The resulting lack of confidence in the protection of personal or privileged information in foreign jurisdictions may adversely affect international trade.

Cross-Border Co-operation in the Enforcement of Laws against Spam

47. New technical means of communication, such as e-mail messaging, have also exacerbated the problems posed by unsolicited commercials. Unreasonable amounts of unsolicited communications have led most large organizations to use filters to block communications from unknown originators, so as to avoid having their servers burdened by unwanted data. That, in turn, has created other problems, such as unintentional loss of commercially relevant information caught by and left unnoticed in quarantine mailboxes in connection with server filters.

48. A number of countries have adopted legal instruments to combat spam. The first problem confronting anti-spam legislation is a definition of and delineation between legitimate commercial messaging and undesired spamming. Enforcement of legal anti-spam measures has proven problematic, due to the number of enforcement agencies and the variety of their powers, limitations on gathering information and sharing information as well as producing the necessary evidence, and limited enforceability across borders due to lack of national jurisdiction over

cross-border spam and of appropriate measures for cross-border enforcement at the operational level.

49. On 13 April 2006, the OECD Council adopted a Recommendation on Cross-Border Co-operation in the Enforcement of Laws against Spam. The OECD Council recognized, inter alia, that spam "undermines consumer confidence," and can facilitate "the spread of viruses, serve as the vehicle for traditional fraud and deception as well as for other Internet-related threats such as phishing, and that its effects can negatively impact the growth of the digital economy, thus resulting in important economic and social costs." The OECD Council further recognized that spam poses unique challenges for law enforcement in it is a "uniquely international problem that can only be efficiently addressed through international co-operation."

50. Against that background the OECD Council recommended that its member countries should work to develop mechanisms for more efficient cooperation among their spam enforcement authorities. Such mechanisms should include, where appropriate, a domestic framework that included: (a) appropriate laws dealing with spam; (b) steps to ensure that spam enforcement authorities have the necessary powers to obtain evidence sufficient to investigate and take action in a timely manner against violations of anti-spam laws that are committed from their territory or cause effects in their territory; (c) improved ability of spam enforcement authorities to take appropriate action against senders of spam and individuals or companies that profit from the sending of spam; (d) periodical review of domestic framework and take steps to ensure their continued effectiveness for cross-border cooperation in fighting spam; (e) ways to improve redress for financial injury caused by spam.

51. As regards international cooperation, the OECD council recommended: (a) providing spam enforcement authorities with mechanisms to share relevant information with foreign authorities; (b) enabling spam enforcement authorities to provide investigative assistance to foreign authorities, in particular with regard to obtaining information from persons; obtaining documents or records; or locating or identifying persons or things; and (c) designating a contact point for cross-border cooperation.

52. The OECD council further recommended that member countries should encourage participation by private sector and non-member economies in international enforcement cooperation efforts; efforts to reduce the incidence of inaccurate information about holders of domain names; and efforts to make the Internet more secure.

53. The Commission may wish to take note of the work being done by OECD in the area of cross-border cooperation in the enforcement of laws against spam. The Secretariat will continue to follow these issues, in particular the relationship between the goal of preventing unsolicited commercial communications and the reasonable commercial use of advertisements and other forms of general business communications in well established business practices.