Promoting e-Commerce in Developing Countries

2

Guilherme Alberto Almeida de Almeida
Alfonso Avila
Violeta Boncanoska

Internet Governance and Policy Discussion Papers

DiPLO
www.diplomacy.edu

Promoting E-Commerce in Developing Countries

Guilherme Alberto Almeida de Almeida, Brazil
Alfonso Avila, Mexico
Violeta Boncanoska, Macedonia

March 2007

DiPLO
www.diplomacy.edu

Acknowledgements

We are grateful for all the support we have received whilst researching and writing up this paper. Special thanks go to our supervisor Marsha Guthrie and our External Supervisor Latif Ladid for their guidance and knowledge. We would also like to express our gratitude to Hannah Slavik and Steve Slavik for their enriching comments and corrections.

Abstract

This study examines the advantages and possibilities for the use of digital signatures to carry out electronic transactions. It focuses on developing and transition countries that have not fully implemented the use of digital signatures in their economic, commercial and productive processes. An important aim of this research is to create awareness on the likely effects for enforcing the use of digital signatures to carry out e-commerce transactions on the economies of developing and transition countries. The study also proposes key issues to be considered for policy-makers in countries in order to consider in fostering the development of e-commerce.

Introduction

As of September 2006, over 1 billion people (or 16.7% of the world population) had access to the Internet (Miniwatts Marketing Group, 2006). World usage has increased by over 200% between 2000 and 2006. Yet, in developing countries, usage rates are significantly lower than in developed countries. Since 1995, the economic consequences of the Internet and related technologies have increased dramatically, resulting in a wide variety of new names such as the "weightless economy" (Quah, 2000) or the "knowledge economy" (Smith, 2001).

The technologies designed to improve commercial transactions using the Internet have evolved as quickly. However, we have not yet achieved an ideal world of painless and secure transactions utilising the Internet, as unresolved privacy issues of the purchaser have impeded the further development of the technologies. During the last dozen years, e-commerce practices have changed in developed and developing countries. For instance, developing countries have fallen behind in the early stages of technology acquisition because of inefficient use of related knowledge, lack of investment within firms to acquire technology, lack of promotion policies that develop these technological areas and high costs of importing technology. Moreover, recent technological developments such as the introduction of digital signatures may widen the gap in the use of e-commerce technologies. Therefore, it is important to examine the perspectives of developing and transition economies with regard to the likely enforcement of digital signatures in carrying out e-commerce transactions.

This is an important issue related to the expansion and promotion of e-commerce in developing countries. The purpose of this paper is to review the situation of several developing and transition countries in relation to the implementation and enforceability of digital signatures in e-commerce transactions. Another important goal of this paper is to create awareness in different stakeholders related to the use, development, and enforcement of digital signatures to carry out e-commerce activities.

Initially, we describe the methods and information used in this study. Subsequently, we deal with factors hampering the development of e-commerce processes in developing and transition countries, which opens our discussion of pre-requisites for successful e-commerce activities. In detail, we analyse the legal and regulatory frameworks for the promotion of ecommerce in developing countries. We then analyse the introduction, use, and enforcement of digital signatures as well as their likely implications for developing and transition countries. Finally, we propose a set of recommendations that may assist different stakeholders (policy-makers, national government institutions, and international organisations) in the development of successful policies and strategies oriented to harness the benefits of e-commerce technologies.

Indicators Dataset

The collection of information for this review required the assembly of an indicators dataset from the Economist Intelligence Unit (2006) (EIU) summarizing e-readiness for several countries. A number of other publicly available information and communication technology indicators from Internet sources also illuminate the processes examined in this study; these indicators were gathered from the International Telecommunications Union, the Organization for Economic Cooperation and Development, and Netcraft. The EIU indicator analysis is based on e-readiness rankings developed by the EIU in 2005, and it uses a scale from 0 to 10 to indicate increasing e-readiness for commercial transactions. Using the EIU indicators simplifies the analysis of data and also shows the level of preparation of some developing and transition countries with regard to the utilisation of Internet technologies, in comparison with the more developed nations. Unfortunately, no indicators are available related to the development or implementation of digital signatures in developing countries.

E-commerce Indicators Analysis

The highest-ranked areas of the world in terms of e-readiness are North America, Western Europe, and some countries in Asia. On the other hand, the bulk of the countries with lower levels of e-readiness are located in developing and transition regions. Figure 1 depicts this information, where each sector of the circle indicates the degree of development of a number of "readiness indicators" (such as "connectivity," "business environment," and others listed in the legend in Figure 2) used to assess readiness.

Figure 1. 2005 World Rank Region E-Readiness

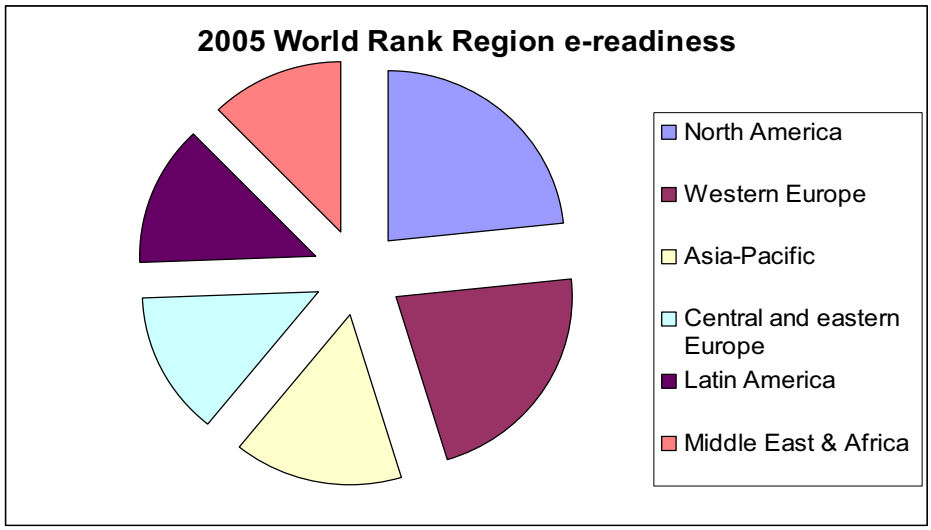


Figure 2 depicts the e-readiness of ten selected countries, the most developed of which is that of Denmark (other Scandinavian countries are similar). Most developing and transition countries lag behind. For example, Russia, Saudi Arabia, and Nigeria clearly fall behind Denmark and Germany. Likewise, China and India, due to the size of their populations, are not well developed in all the categories that the e-readiness indicator considers. However, their positions are improving continuously. Special cases can be found in South Korea, Chile and, to some extent, in Mexico; these countries have made some progress in improving their e-readiness.

Nevertheless, their positions within the e-readiness ranking are far from the Scandinavian countries. When examining e-commerce indicators, one observes that mobile payment methods are increasing in number; in 2002, a third of the new payment schemes recorded by the Electronic Payment Systems Observatory used a mobile platform (OECD, 2006). In Japan, individuals use mobile phones more frequently for payment than personal computers. Mobile payments are also used in other countries, including Finland and Korea, though other payment methods are preferred. In Africa, the large number of mobile devices has increased the number of mobile payments and transactions. However, not all mobile payment systems have been successful and the preferred method of payment within countries in the OECD area is still the credit card, followed by the debit card and e-banking transactions, as Figure 3 indicates. A similar picture likely occurs in developing and transition economies.

In addition, security is a sensitive issue when discussing e-commerce. As Figure 4 illustrates, however, the number of secure servers of some developing and transition economies is continuously increasing. The most important thing to note about the change in the number of secure servers is that these developing and transition countries have not yet developed the technological infrastructure to compete with the most developed countries in terms of e-commerce. South Korea is the most developed country, which is perhaps an indication of previous technological investments.

Figure 2. E-Readiness Indicators for some Developed, Developing and Transition Economies - 2005

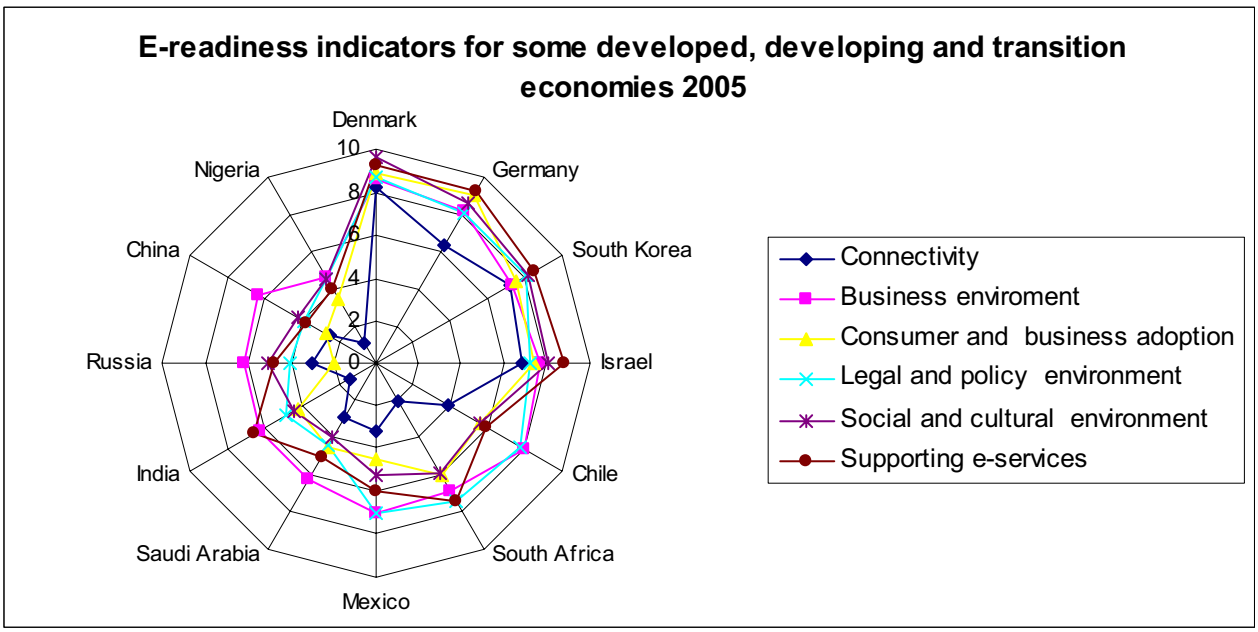
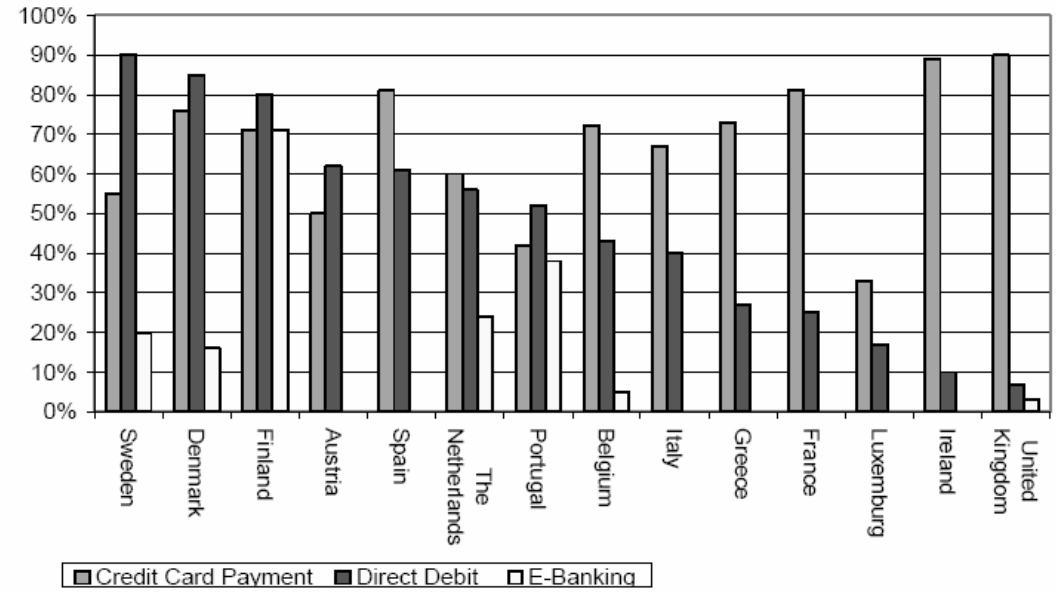
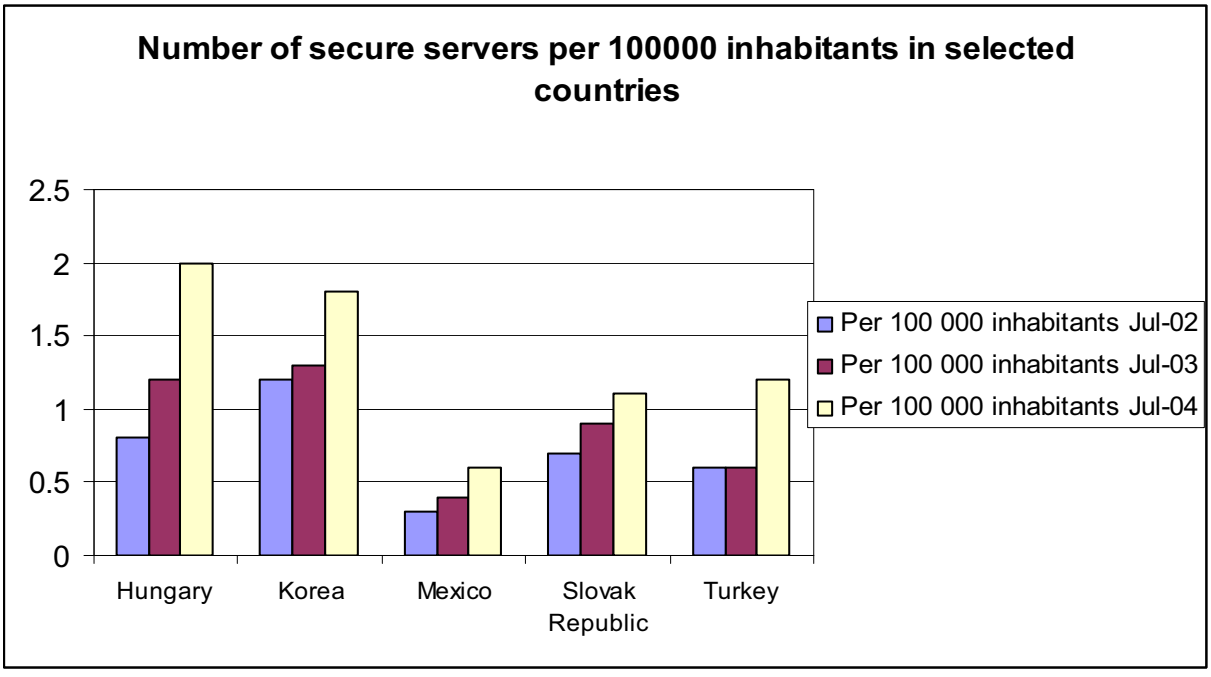


Figure 3. Payment Methods Most Frequently Proposed by e-Commerce Websites



Source: OECD 2006

Figure 4. Number of Secure Servers per 100,000 Inhabitants in Selected Countries



Source: Netcraft 2005

Factors Hampering Growth of e-Commerce in Developing Countries

A number of factors have hampered the growth of e-commerce in developing countries. Yet, the main perceived obstacle to increased Internet usage is very similar in companies from both developed and developing countries. Firms already using the
Internet consider the lack of network security to be the primary problem, followed by slow and unstable connections. Lack of technical skills is not the only reason preventing firms from going online. However sometimes company owners lack knowledge management on Internet and ICTs in general. (Gwyer, 2004; UNCTAD, 2004). Furthermore, various impediments are responsible for the current limited use of e-transactions by small- to medium-sized enterprises.

Among many potential users, a serious lack of confidence in e-commerce impedes usage. For this reason, firms make complementary usage of video conferencing and other communication methods such as telephone, e-mail, and face-to-face communications. A scarcity of information technology administrative systems and a lack of experience make firms hesitate to utilise e-commerce fully to digitize all of the administrative works related to business transactions. High costs and fees to start e-commerce by utilising e-marketplaces are a severe hindrance, especially for enterprises incapable of developing their own systems. Insufficient human resources and digital infrastructure are always concerns when one discusses development of smallto medium-sized enterprises (Kuwayama, 2005). As discussed by Mansell (2003) and Hawkins (2000), large corporations carry out the bulk of e-commerce activities. However, during the last eight years a constant and important growth of ecommerce transactions by small- to medium-sized businesses, individuals, and governments at different levels must be considered. Same study claims that business-to-business e-commerce does not offer greater returns to firms in developing countries than other channels for conducting trade. Accordingly, it is mandatory that firms in developing and transition economies accomplish some initial requisites successfully to carry out e-commerce processes.

As an illustration, we can mention the case of many African countries. Improvement and change are essential if Africa is to become fully engaged in electronic commerce. E-commerce is a viable mechanism for linking the entire globe into one “trading centre” without restrictions from territorial and geographical factors. As well, e-commerce is a major channel for offering African countries more options and access to products not produced or traded in the region. E-commerce could help African firms to reduce the associated high costs of doing business in Africa by allowing inter-firm communication at reduced costs, making quick settlement of payments, and mitigating the need to maintain large inventories.

The general state of development of telecommunications and e-commerce on the African continent is still poor, compared to the rest of the world. With only 0.6% of the Internet users in the world, Africa’s minimal goal of readiness for extracting meaningful benefits from virtual commercial transactions has proven elusive. The electronic commerce leader within Africa is South Africa, whose Internet users constitute two-thirds of the continent’s total Internet users, and whose overall level of ICT development is considerably ahead of the rest of the continent. In 1999, consumer-to-consumer e-commerce in South Africa was estimated to total US$447 million, while business-to-business e-commerce totalled about US$663 million (ITU, 2001).

Pre-Requisites for Successful E-Commerce Growth

In order to attain a successful level of e-commerce development, firms in developing and transition economies must attain some initial levels of trust in e-commerce, of ICT infrastructure, and legal and regulatory frameworks.

Building trust

Building trust or confidence is a precondition for doing e-commerce in developing countries. Without trust or confidence, the very effort of promoting e-commerce in developing countries would be fruitless. As explained by Bacchetta (1988) in a World Trade Organization study, only if buyers and sellers trust that orders and payments are conducted with minimal risk of deceit and abuse of any information provided, will they accept the Internet for electronic commerce purposes. Buyers and sellers will only take the risk of making contractual obligations over the Internet if they know their rights and obligations and that these will be enforced.

The promotion of trust and confidence depends on a number of factors. Goldstein and O'Connor (2000) pointed out that e-commerce requires legal norms and standards covering, for example, contract enforcement, consumer protection, liability assignment, privacy protection, intellectual property rights, and process and technical standards. For example, standards regarding the way payments are accepted on the Internet and products are delivered to the final user, regarding security, authentication, digital signatures, and connectivity protocols are required. As Goldstein and O'Connor (2000) underlined, trust is also necessary at many levels, including hardware and software security, the regulatory regime, familiarity and users' perceptions. They noticed that in developing countries, trust is established and reinforced through family association and subsequent, repeated personal contact and interaction. In western countries, the trust is set up through impartial enforcement of law and its adaptation to a new technological environment. As a result, where legal and juridical institutions are underdeveloped, as in much of the developing world, e-companies find themselves at a disadvantage because of insecurity, whether real or perceived.

Common e-commerce security controls include authentication, access control, encryption, firewall, intrusion detection, anti-virus software, and spyware (Businesslink, 2006). Moreover, trust-building tools (such as VeriSign and BBB online certifications) may help e-companies in the developing world. Furthermore, before entering into a commercial arrangement with a stranger, access to information about credit history, annual turnover, and previous trading associates would be desirable. Firms could then judge the legitimacy and creditability of a potential trading partner. These preconditions are also applicable for building trust in e-marketplaces (Mansell, 2003). However, even were trust and confidence are present, the adoption of e-payment technologies would require a number of ICT infrastructure measures related to the development of e-commerce transactions.

Measures Necessary for Adoption of E–Payments in Developing Countries

The 1990s saw the mainstreaming of electronic commerce, which takes place with a buyer initiating a transaction by computer over the Internet or proprietary network (Visa International, 2002). However, e-payments necessitate systems and procedures for paying electronically and their existence is "a precondition for the successful development of e-commerce" (Kurbalija and Gelbstein, 2005).

In general, if users feel comfortable in making transactions online, they can save time and money. E-payments directly support business growth and, according to some macroeconomic visions, annual savings of perhaps 1% of GDP can be realised, if a country is able to shift from an all paper-based to an all electronic-based payment system. However, bearing in mind the sensitivity of money and payment-related issues, the potential benefits are hardly achievable. Digital cash and low technology penetration creates problems in developing countries due to lack of trust in online transactions together with their questionable security. These are major obstacles to the wide acceptance of e-payments. Electronic money (also known as electronic cash, electronic currency, digital currency, and digital cash) refers to money exchanged only electronically. Typically, this involves the use of computer networks, the Internet, and digital stored value systems. Electronic funds transfer and direct deposit are examples of electronic money (Mansell and Steinmueller, 2000).

The customer loads electronic cash or digital cash from his bank on his computer or onto his smart card. A Trust Centre verifies digital cash and it is valid only if it is produced along with a certificate. At each transmission of the electronic cash, its validity needs to verification by the Trust Centre. The owner of the electronic cash can get real money in exchange for digital cash, provided it is properly authenticated.
Developing countries have far to go to implement e-money systems successfully. First, digital cash is a threat to every government that wants to manage its own currency. Second, governments are concerned about the potential use of e-money for money laundering (Kurbalija and Gelbstein, 2005). Third, lack of security, privacy, and customer trust remain as impediments to the implementation of e-money, as well
as impediments to overall e-payment acceptance. According to Goldstein and O'Connor (2000), factors affecting the level of trust required and provided in regard with e-payments include:

- Where and how payment takes place (real or virtual settlement)
- When settlement takes place (prior to, at the time of, or after the transaction)
- Who settles it (established incumbents or new entrants)
- Whether the transaction is business-to-business or business-to-consumer (with online settlement much less advanced in the former than the latter)
- Whether settlement can be traced.

However, more importantly, ICT infrastructure must be available to support all of these factors. In addition, the Information for Development Program (2006) encourages cash-free payment, claiming that "elimination of physical cash has many advantages including less opportunity for fraudulent or criminal activity, reduction of cash handling costs and, for the user, less reliance on having the right amount of cash when needed." The same report also shows that now large numbers of prepaying users frequent developing markets, users very familiar with using their phones for text and voice messaging, as well as with refilling their credit balance on the prepaid system, this same group is an ideal segment to target with a micro-payment feature.

In many cases they have no relationship with any bank, do not use electronic funds transfer at Point of Sale or credit cards and yet they have the ability to perform financial transactions as evidenced by their ability to purchase and activate prepaid cards for additional credit.
An Arthur D. Little study (2004) points out that the success of payments made by mobile devices depends on establishing partnerships and defining clear roles and incentives across the value chain. The sooner the players are able to co-operate on developing mobile payment standards, the faster they will take hold and bring benefits to all involved in the value chain. A trusted brand is critical in generating confidence in mobile payments and achieving critical mass of customers and merchants. Finally, an important success factor for companies investing in mobile payments is to achieve a critical mass of customers. Additionally, Heng (2004) suggests that mobile payment systems have a great advantage over Internet-backed services in terms of access conditions, in that they are used in both online and offline transactions.

Nevertheless, mobile payment services are subject to limitations, as they connect via mobile phone, a medium unsuitable for higher-level security demands. Hawk (2002) presents indicates that Russia, India and Brazil have developed some alternative payment methods in business-to-commerce e-commerce systems, such as cash on delivery (paid to the courier or delivery service), bank and wire transfer, cheques, and demand drafts.

Legal and Regulatory Frameworks for the Promotion of e-Commerce

It is necessary to allow users and further players in the market to gain confidence in the use of ecommerce solutions. This may be done not only by the use of adequate technologies to ensure technical security (thus preventing fraud, information leaks, and other forms of attacks), but also by strategic initiatives aiming at a change in user perspectives on the reliability of ICT in commercial transactions. Legal and regulatory development acts as a possible pre-condition for the promotion of such confidence.

In fact, commercial activities usually depend on laws that regulate the execution of contracts, their validity conditions, their enforcement, their limits of liability, and their resolution in case of conflict. In all cases, a clear scenario is required to allow commercial players and consumers to have a clear view of the implications of the transactions performed. The shift from regular commerce to e-commerce has raised several questions regarding the applicability of existing laws to such new forms of trade, as well as regarding the promotion of new regulations to recognize new methods of communication and transactions embodied therein. Particular attention has been directed to the issue of digital certification, a technical mechanism to ensure the validity and security of electronic transactions. In addition, so long as e-commerce is intrinsically international, harmonization of local regulations concerning these issues has been prompted.

Non-discrimination. An initial step in the recognition of electronic means as valid and enforceable in connection with commercial transactions consists of expressly accepting such means as a possible and legally binding method for such transactions. This recognition leads to a "non-discrimination" principle, through which it is accepted that the use of electronic means to transmit information or to express the acceptation of a certain agreement should not be used to discriminate it from regular non-digital transactions, as if such e-transactions would be intrinsically void. Assuming that transactions may be performed by electronic means leads to further regulation of specific digital procedures to ensure that such procedures would have the same practical, legal, and functional effects that regular non-digital procedures have. Such goal may be attained by the principle of Functional Equivalence.

Functional equivalence. One of the primary concerns in respect to e-commerce has been to define how transactions executed by electronic means might have the same validity levels of contracts executed by regular, paper-based, agreements. Most prior, local or even international regulations have been worded in a sense that important elements (such as "signature" or "original") correspond to realities of a non-digital environment.

The mere interpretation of such legislation as automatically applicable to new digital realities could lead to inconsistencies: in most cases, specific non-digital procedures and concepts are acknowledged by law or regular practices based on the specific effects they produce. A clear example in the case of signatures is that in a paper document, a signature may evidence, at the same time, (i) the identity of the person who signed it; (ii) that such person has approved or authored such document, as the case may be, and even (iii) that such document has not been altered (it is a regular practice, in some countries, to sign all pages of a document, as a way of preventing fraud through the alteration of initial pages).

Therefore, the transition from paper-based to digital procedures, from a legal perspective, will depend on the recognition of the functions performed by some non-digital procedures and by the development of equivalent digital procedures that lead to the same results. In order to ensure that digital transactions are trustworthy, it is necessary to ensure that digital procedures should be as trustworthy as their non-digital correspondents, and to have them recognized by law.

Technological neutrality. Technological neutrality or technological independence is often mentioned as a principle for the drafting of adequate ICT legislation and regulation. Koops (2006), despite his critical view of the technological neutrality principle, clarifies some of the different possible interpretations of such a principle. According to Koops (2006), statements of technological neutrality could be interpreted from at least three different points of view: concerning the purposes, consequences, and legislative techniques of such regulation. Each perspective may lead to different possible interpretations concerning the purpose of the regulation, concerning the consequences of regulation, and concerning the legislative techniques involved.

The Introduction, Use, and Enforcement of Digital Signatures

The United Nations Commission on International Trade Law (UNCITRAL) (1999) formulated a model law that develops a legal framework for digital signatures. This model law, called the UNCITRAL Model Law on Electronic Signatures, defines electronic signatures as data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message. This definition stipulates the three main aims of e-signatures, which are the electronic form of the signature, the identification of the signatory, and the non-repudiation of the signature, ensuring effectively that the signatory cannot later refute having signed the document. The Model Law establishes three requirements for a digital signature.

First, it establishes that electronic signatures are legally valid only if the signature data is undoubtedly linked to the signatory and no one else. Second, it requires that at the time of creation, such data were under his sole control. Third, it demands that any alteration made to the electronic signature must be detectable.

Once these three articles are confirmed, then additional legal requirements for a signature may be put into place by the country wishing to adopt such legislation. Currently, it is important to differentiate clearly the expressions "electronic signatures" and "digital signatures," often used synonymously, causing unwanted ambiguities. "Electronic signatures" is commonly used in accordance with the context of the UNCITRAL Model Law. "Digital signature" is closely related to the specific technology for electronic signatures based on Public Important Infrastructures and asymmetric cryptography, which has been the main technology used in the implementation of "advanced" (or qualified) electronic signatures. The importance of establishing a common international framework for electronic signatures remains evident from a legal perspective.

Inasmuch as the development of electronic means of communication may promote a more rapid and more efficient way of business, the intrinsic nature of the digital sphere (i.e., the lack of physical contacts, the possibility of interception, mass copying, or adulteration of electronic documents, the uncertainty of identification and authorship) represents a clear factor for potential lack of confidence.

Therefore, based on the functional equivalence principle, electronic signatures appear as a mechanism that, by law, may be acknowledged as valid and efficient to promote the same effect of paper signatures, or at least to allow electronic documents admission as evidence in legal proceedings. Therefore, the recognition of electronic signatures plays an important role in increasing e-trust for companies willing to perform its digital activities, ensuring the possibility of having electronic documents that would not have their validity rejected by courts.

Functioning of Electronic Signatures

The UNCITRAL definition for electronic signatures permits a wide interpretation. In fact, the use of a login or password scheme, or even a personal identification number for a banking card, may be interpreted as data in an electronic form logically associated with other electronic data, serving as method of authentication. In this sense, within a legal context, a broad range of technological solutions may be used in order to ensure that electronic data be used as evidence of negotiations or contracts by electronic means. Electronic signatures work differently from paper based signatures, as long as the former relies on electronic means of verification.

Electronic signatures depend on the existence of a "certificate" that stands as an electronic record that links the signatory to his or her signature (or, in most cases, to signature-verification data). It is important that such a certificate be issued by a reliable entity usually known as a "certification service provider," or a "certification authority." Stronger confidence and, therefore, legal validity may be obtained if such certification service provider takes significant measures to ensure the reliability of the link between the signatory and his or her signature-verification data.

We stress that some particular characteristics of the so-called "advanced electronic signatures," which are electronic signatures with a stronger level of recognition by legal systems, should be based on "qualified" certificates. Qualified certificates meet certain technical, informational, and logical requirements, and are provided by certification-service-providers that meet certain technical, financial, and procedural reliability requirements). These certificates are created by "secure-signature-creation devices" (i.e., signature creation devices that meet some technical and procedural requirements, such as ID verification).

In general, advanced electronic signatures grant the same effects as paper-based signatures. In practice, advanced electronic signatures require a trusted third party (the certification service provider) with strong security procedures, reliable implemented technology, and large financial liability for damages. Therefore, it represents a higher-cost solution to end-users, with stronger or, in most cases, directly enforceable legal validity. Commonly, advanced electronic signatures correspond to digital signatures based on Public Important Infrastructures and asymmetric cryptography and provide extra advantages from a practical point of view.

Potential Applications of Electronic Signatures

Electronic signatures usually depend on recognised secure electronic transaction methods. Therefore, the use of such security tools may improve e-confidence by practical and legal means. In some cases, the use of electronic signatures may foster the implementation of automated transactions. In fact, proposed and in-force legislation usually ensures stronger legal validity of technological procedures that promote high degrees of integrity and authenticity of a document. Security and legal validity, therefore, remain as different aspects of building confidence for electronic commerce. Certificates may be issued not only to individuals, but also to entities such as companies, or even websites. Business-to-consumer transactions, for instance, could be held on secure and authenticated environments, in which a transaction would result in a legal and enforceable document. Likewise, electronic signatures are also quite relevant for e-payments. Both security and legality encompassed by e-signatures allow that cash flow, more than only e-documents, be formally transmitted by electronic means.

Another important advantage concerning the use of advanced electronic signatures in particular is that an asymmetric cryptographic structure allows reliable encryption of documents transmitted by the Internet. The use of attribute certificates may, therefore, be of great help in the development of confidence in e-business. It may stand as a financial credential before third parties, issued by financial institutions. It may also work as a trustworthy certificate issued by a relevant intermediary, therefore promoting trust in e-negotiations.

Potential Conflicts in e-Commerce and Electronic Signature Regulation

As we have seen, regulating e-commerce and electronic signatures plays an important role in promoting e-confidence. However, the development of non-harmonic legislation may cause some compatibility problems on a global scale. As well, insisting on certain security and legal practices may cause negative economic effects on e-business.

Cross validation and recognition. The UNCITRAL Model Law on Electronic Signatures states that certificates issued outside a certain country shall have the same legal effects as domestic certificates, if such foreign certificate offers a substantially equivalent level of reliability. Such provision seeks to harmonise the legal validity of electronic documents, but may raise conflicts in case of countries that decide to establish regulations that are more stringent, due to internal political or economic concerns.

For instance, some countries may require that certification authorities determine severe technical and procedural policies for the issuance of certificates. In addition, some countries require certification authorities to contract liability insurance covering concerning potential damage to users. Such requirements may be the cause for the non-recognition of legal validity to certificates issued outside a certain country's territory. Such problems may be solvered by cross validation recognition instruments, but also by stipulating minimum requirements.

Costs. The definition of advanced digital signatures as the standard for full validity of electronic documents may generate further costs for the development of e-commerce. Despite their function of ensuring that legal trustfulness should arise out of technological confidence, qualified ctificates depend on technological, procedural and infrastructure requirements that may significantly augment implementation costs. As a consequence, less-expensive, yet almost as trustful security procedures may be neglected. Further, the high costs of such certificates may minimise their penetration among small- to medium-sized businesses, thus either hindering the development of new e-business solutions for this sector, or promoting alternative validation methods and procedures with lesser legal support.

Cultural Issues. Finally, it is worth mentioning that, just like any other specific technology, the use of electronic signatures depends on certain training and culture building. Specific tools for using the technology already exist, and most operating systems–but not necessarily all–are ready for its use and recognition. However, the implementation of advanced electronic signatures on a bigger scale will demand extra costs in training, software, hardware, and will certainly face some initial cultural opposition during its implementation. Such negative effects could be minimised by drawing special attention to training and education for its functioning structures, forms of use, intrinsic benefits, and legal consequences of misuses.

Implications for Developing Countries in Use of Electronic Signatures

The UNCITRAL Model Law establishes and promotes the use of Public Important Infrastructures and advocates developing countries to develop electronic signature and certificate legislation. The UNCITRAL Model Law is important for the homogenising process, since electronic signatures are part of the international electronic commerce phenomenon. That is, if electronic trade is to develop then it is important that legislation in this area have the same foundations in all countries. However, UNCITRAL does not enforce the use of digital certificates and signatures.

Therefore, the most important players at a global level, those characterised by mergers of software developers and financial institutions, are promoting the legislative process in many developing countries. In order to further follow the remainder of this discussion, four issues need explanation: the absence of technological standards with providers of digital certificates and signatures; the lack of information and awareness among many of the likely stakeholders involved in enforcing the use of digital signatures; the cost of signatures varies with the encryption technology used; and the absence of a consistent and reliable legal framework First, providers of digital certificates and signatures have no technological standards. In fact, for each of the crypto-technologies different firms seek a monopoly in providing the relevant technology. For instance, in the case of passwords, VISA and MasterCard take the lead. In face-recognition firms, Crypto and Faceoptics push these developments and DNA recognition is developed by DNAimportant and DNASource. Moreover, no agreement regarding the best authentication technologies exists. Currently, different technologies carry out electronic transactions (see Appendix 1). All technologies have shortcomings and advantages. Further, even though no authentication standards exist, many countries taking the first steps towards the creation a framework allow the enforcement of digital signatures.

Second, many of the stakeholders involved in the process of using digital signatures lack information and awareness. For instance, in some developing countries, the process has been started with the use of digital certificates to declare and pay taxes. In this process, the government enforces the use of digital certificates for tracking the taxes of registered taxpayers. One digital certificate is given to each registered taxpayer. Although issuing a digital certificate is very costly (around US$170), the government and other stakeholders are subsidising this technological investment that will result in the collection of higher levels of taxes. These certificates can then be used with a system of digital certificates, certificate authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction. However, no single standard has been established for setting up the infrastructure. Third, the price of the signatures varies depending of the encryption technology used and the size of the provider. For example, a digital password provided by Visa or MasterCard costs nothing or almost nothing to the customer; the cost is absorbed by the credit card corporation. Yet, if the customer wants a signature acquired from a firm or from one of the firms a government has assigned for the provision of these certificates (as is the case in Brazil), then the cost may go up to US$150. In this way, an unfinished commercial fight between signature or certificate providers may result in a standards war.

In addition, the UNCITRAL Model Law does not guarantee at all that in twenty years more sophisticated digital signatures will not be necessary, that is, that the digital signature with standards of 2005 will still be used. Therefore, if an individual paid a sum for a certificate in 2005, then, he may need to pay extra for acquiring the new technology (lets say, based on DNA or iris recognition) to carry out secure electronic transactions. Indeed, this is one of the biggest problems facing the enforcement of digital signatures.

It is initially easier for a firm to acquire this signature certificate because it will be used for a company with more purchasing power than that of an individual. More importantly, in case the digital signature is subsidised by the government, the taxpayer will pay more in the future for the update of digital signature technology.

Fourth, no consistent and reliable legal framework exists within which to enforce the use of digital signatures in developing and transition economies. Although international and regional efforts exist to establish frameworks and rules for digital signatures, electronic security, and payment systems, these measures do not appear to be crucial for most types of business-to-business e-commerce currently practiced in developing countries. In fact, very little on-line buying and selling of developing country producer firms' products is found (Mansell, 2003). Contract commitments and payments are not generally made on-line. Conventional commercial practices in these areas are favoured by firms, even those that find buyers or suppliers through business-to-business e-marketplaces. Therefore, the emphasis of business-to- business e-commerce policy on developing legal frameworks for online trading (e.g., digital signatures and electronic trust services) is questionable. Furthermore, no indication shows that radical new business models would emerge if these legal issues were resolved.

In sum, it is suggested that the use of digital signatures would expand if:

1. Security aspects of the process were improved
2. The process and technology were extended to facilitate common business practices that fall outside the limited realm of current digital signature capabilities
3. The cost of the acquisition of technology was lower
4. Correctly and fully informed stakeholders made adequate decisions.

A Regulatory Framework Fostering the Development of e-Commerce

Proposals and strategies to promote successful e-commerce processes have been created in developing and transition economies, such as Mexico, Brazil, Kenya, South Africa, and the Philippines. In some countries, a two-tiered strategy has occurred. Either they created proposals because they joined the European Union or a larger community of countries, or they developed them following the example of other countries in the area or pushed by international organisations.

Improvement of Access to Information on International Trade

A pressing need to develop ICT infrastructure exists, especially in less developed countries. Among Internet users, information sharing, retrieval, and collection are the main uses of the Internet. Once firms obtain Internet access, they can benefit from these processes. "One-stop service" or establishment of a portal site is the best way to improve information access. What is important is to design the portal from the users' standpoint. A portal site specialised in a specific industry, or a Vertical Portal, is often helpful.

Capacity Building

Lack of preparedness, awareness, and the need for training are very important issues. The need to build capacities in ICT use and general capacities in the industrial sectors of developing countries is outstanding. Competence in ICT is becoming a prerequisite for inclusion in global value chains. On-line buying and selling may not be developing, but a clear growth is seen in on-line co-ordination of supplier-buyer relationships. Capacity building and training are crucial for operating in international markets, but the contribution of business-to-business e-commerce requires careful definition. Capacity building initiatives need governance by the context in which producer firms are operating in international markets (Mansell, 2003). Foreign language and business culture are also recognised as important areas of capacity building.

Formation of Virtual Clusters

Group cooperation among small- to medium-sized enterprises can be an effective scheme to foster export industry and promotion. It enables small firms to achieve scale economy and enhance bargaining power. These benefits make it feasible for these businesses to invest in ICT and involve themselves in e-commerce. In the near future, these groups will find business opportunities from forming Internet-based network business groups that are more flexible than traditional pyramidal supply chains composed of a large firm on top of the first- and lower-tier suppliers. With the network type association based on the Internet, it is possible not only to network firms placed within an industrial accumulation but also to create a "virtual cluster" that links up with cooperative networks in different regions.

Trade Facilitation

Burdensome trade-related procedures are substantial barriers for small- to medium-sized businesses to export their products. Inefficient handling of trade-related documents overseen by governmental departments raises the total cost of international trade. Trade facilitation requires extensive countermeasures against these problems. The subjects to be examined are, for example: improvement of access to information on trade-related policies and regulations; simplification of trade-related procedures; mutual recognition of sanitary measures; digitalization of trade-related procedures such as customs clearance, sanitary measures, and certificates of origin; and establishment of "single window systems" that interconnect various computerised systems related to international trade and transportation.

Improvement of Infrastructure for e-Business

Harmonisation of business rules based on legal and dispute-settlement systems and common technical standards are required to facilitate international e-commerce. The governmental sector can provide businesses with incentives and opportunities to gain experience with electronic transactions by computerising tax collection, public procurement, and other public services. Moreover, additional recommendations would show how to promote ecommerce further in developing countries.

Issues to Consider in Developing Successful Policies in e-Commerce

This study cannot present a full proposal for promoting successful e-commerce transactions in developing and transition economies for several reasons. First, each country may have a different stage of development with regard to the legal and business framework where this kind of policies may fit. Second, each country has an asymmetrical development of technological and socio-economic factors. Hence, each policy or strategy must be customised to the particular situation of each country. Therefore, this study will propose a set of issues for a policy-maker to consider when he or she faces the creation of such policies. First, a process of awareness should be created and implemented by the government, technology providers, educational institutions, and other stakeholders to inform the general public about the likely implications, impacts and effects in creating such policies. No other policy or recommendation should be considered or started if the awareness process was not carried out successfully.

- Develop a dialogue to discuss these issues within a diverse, large, and informed community of stakeholders.
- Deeply examine and assess the available technologies to be used, including their obsolescence.
- Develop a foreseeing scenario of which technologies will be in use (with regard to e-commerce) in the next ten years.
- Fully assess the providers of the technology, procedures, and the transfer to local firms and institutions.
- Assess the implications and effect of the implementation of these technologies in different industries.
- Develop the necessary human capital capacity in order to successfully transfer the technology to local developers.
- Create a bid process for technology acquisition to include as many technology providers as possible and to reduce the price of the technology.
- Allow adequate time for a legal framework to be developed and enacted.
- Seek advice of international organisations and institutions with authority in the issues.
- Investigate who will buy digital signatures, how many owners there will be.
- Observe the patterns followed by developed countries with respect to the enforcing of digital signatures and learn positive and negative aspects. Moreover, if stakeholders decide to continue with the process and enforcement for the use of digital signatures-certificates is established, then it is necessary to consider the following aspects.
- Establish domestic controls on the use of encryption technologies as well as on their import.
- Define the role of the government in encryption processes (as a certifying entity).
- Create a transparent process of technology licensing with respect to digital signatures with international standards.
- Carefully examine the UNCITRAL model law on digital signatures.
- Modify the civil code and include the legal definition of electronic data messages.
- Create laws that fully protect the rights of the consumers utilising these new technologies.
- Develop substantial amendments to provide that all kinds of information generated from technological means (electronic, optic, and any other kind of technology) will be considered valid evidence.
- Emphasise that agreements entered into through technological means and, in general, depend on technological resources will be valid only when they comply with evidentiary requirements.
- Ensure that amendments to digital signatures will acknowledge technological means as acceptable for entering into valid, binding agreements.
- Ensure that amendments also set forth the basis for implementing the use of information technology in a Registry's operations.

Much remains to be done by many stakeholders if e-commerce in developing economies is to experience the type of growth evident in more developed countries. As this paper has shown, technology is but one factor among many. Initiatives by governments are beginning to address the usage divide indicated from both a technical and social standpoint.

References

Bacchetta, M. (1998). Electronic commerce and the role of the WTO [online]. Available from: http://www.wto.org/english/res_e/booksp_e/special_study_2_e.pdf [Accessed 19 September 2006].

Businesslink. (2006). E-commerce security issues [online]. Available from: http://www.businesslink.gov.uk/bdotg/action/layer?r.l1=1073861197&r.s=tl&topicId=1073866263 [Accessed18 September 2006].

Economist Intelligence Unit. (2006). World e-readiness report [online]. Available from: http://www.eiu.com/site_info.asp?info_name=eiu_2006_e_readiness_rankings [Accessed 5 October 2006].

Goldstein, A. and O'Connor, D. (2000). E-commerce for development: prospects and policy issues [online]. Technical paper No.164. OECD Development Centre. Available from: http://unpan1.un.org/intradoc/groups/public/documents/APCITY/NPAN004061.pdf [Accessed 12 September 2006].

Gwyer, J. (2004). Has the Internet increased trade? Evidence from industrial and developing countries [online]. Available from: http://topics.developmentgateway.org/trade/rc/ ItemDetail.do~388033 [Accessed 18 September 2006].

Hawk, S. (2002). B2C e-commerce in developing countries: a comparison of India, Latin America and Russia. Proceedings of the 5th International Business and Economics Conference held at St. Norbert College. De Pere, WI: St. Norbert College.

Hawkins, J. (2000). Towards "digital intermediation" in the European information society. University of Sussex. Social Policy Research Unit: Brighton, England.

Heng, S. (2004). E-payments: modern complement to traditional payment systems [online]. Deutsche Bank Research, No.44, May 6, 2004. Available from: http://www.dbresearch.com/PROD/DBR_INTERNET_EN-PROD/PRODOOOOOOOOOOO79835.pdf [Accessed 3 September 2006].

Information for Development Program. (2006). Micro-payment systems and their application to mobile networks [online]. Available from: http://www.infodev.org/files/3014_file_infoDev.Report_m_Commerce_January.2006.pdf [Accessed 21 October 2006].

International Telecommunication Union [ITU]. (2001). Telecommunications indicators database. Available from: http://www.itu.int/publications {Accessed 15 October 2006].

Koops, B-J. (2006). Should ICT regulation be technology neutral? In: B-J. Koops et al. (eds.). Starting points for ICT regulation. Deconstructing prevalent policy one-liners [online]. Available from: http://ssrn.com/abstract=918746 [Accessed 22 September 2006].

Kurbalija, J. and Gelbstein, E. (2005). Internet governance: issues, actors and divides. Valletta, Malta: DiploFoundation.

Kuwayama, I. (ed.). (2005). Information technology for development of small and medium-sized exporters in Latin America and East Asia [online]. Available from: http://www.eclac.org/comercio/IT%5FSME/Documentos/LC-W.27%20-%20Information%20Technology%20Mikio%20final%20ingl%E9s.pdf [Accessed 10 September 2006].

Little, A.D. (2004). Making m-payments a reality [online]. Available from: http://www.adlittle.de/downloads/artikel/MPayment_press%20release_English_Final.pdf [Accessed 13 September 2006].

Mansell, R. (2003). The reality of e-commerce with developing countries [online]. Available from: http://www.gapresearch.org/production/Report.pdf [Accessed 12 July 2006].

Mansell, R. and Steinmueller, W.E. (2000). Mobilizing the information society. Strategies for growth and opportunity. Oxford: Oxford University Press.

Miniwatts Marketing Group, (2006). Internet world stats: usage and population statistics. Available from: http://www.internetworldstats.com/stats.htm [Accessed 22 October 2006].

Organization for Economic Co-operation and Development [OECD]. (2006). Online payments and e-commerce. Paris, France: OECD.

Netcraft. (2005). Netcraft survey 2005. Available from: http://www.netcraft.com [Accessed 12 October 2006].

Quah, D. (2000). Welcome to the weightless world. Centrepiece Magazine, London School of Economics and Political Science.

Smith, K. (2001). What is the knowledge economy? Knowledge-intensive industries and distributed knowledge bases. Working Paper. Maastricht, The Netherlands: INTECH. United Nations Commission on International

Trade Law [UNCITRAL]. (1999). Model law on electronic commerce with guide to enactment (1996) with additional article 5 bis as adopted in 1998 [online]. Available from: http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf [Accessed 22 September 2006].

United Nations Conference on Trade and Development [UNCTAD]. (2003). E-commerce development report [online]. Available from: http://r0.unctad.org/ecommerce/ecommerce_en/edr03_en.htm [Accessed 18 September 2006].

United Nations Conference on Trade and Development [UNCTAD]. (2004). E-commerce development report [online]. Available from: http://r0.unctad.org/ecommerce/ecommerce_en/edr04_en.htm [Accessed 18 September 2006].

Visa International. (2002). Electronic payments, economic growth, and financial efficiency: e finance for development [online]. Available from: http://www. visacemea.com/av/pdf/0302_ucom_white_paper.pdf [Accessed 22 September 2006].

Biographies

Guilherme Alberto Almeida de Almeida

Guilherme graduated from the Law School of the Universidade de São Paulo, Brazil, in 2000. He is presently a member of the Brazilian Bar Association, São Paulo section and a partner of KCP Attorneys at Law, a Brazilian law firm focused on Information Technology and Entertainment Law. He participated in the Internet Law Program, held in Brazil in 2003 by the Berkman Center for Internet and Society, the Getulio Vargas Foundation and the Getúlio Vargas Foundation Information Technology Law Extension Program. He is co-author of the Brazilian published, "Legal Internet – Law and Information Technology" and "e-hints: Devirtualizing the New Economy." He is also author of several articles concerning intellectual property, the Internet, and information technology law. He has been a guest lecturer for several conferences and symposiums held in Brazil and a guest teacher for information technology law in post-graduation courses of Univercidade and Escola Paulista de Direito. He is an academic researcher for information technology related issues.

Alfonso Avila

After finishing his PhD in the UK, Alfonso remained in the UK. Currently, he works for both Sussex and East Anglia universities providing courses related to Economics of Technology and Technology Policy with special focus on ICT. Alfonso also works as a technology policy consultant at an English independent consultancy firm mainly involved in projects related to ICT. The issues he is currently working on relate to e-security in developed and developing countries. He has worked within the ICT area for ten years for various governments (those of the UK, Mexico, the Netherlands, and Spain), various private firms (British Telecom, Lloyds Bank, Hewlett-Packard), and one NGO (DiploFoundation). Alfonso enjoys travelling, reading books on philosophy, learning languages (currently Italian), cooking, cycling, and running.

Violeta Boncanoska

Violeta is a graduate of the University of Ss. Cyril and Methodius, in Macedonia, and currently is finishing an MBA there in the Faculty of Economics. She is finishing a thesis in international management with a focus on "TNC and Technology transfer." She was part of the Diplo Internet Governance Capacity Building Program in 2006 and a Diplo Fellow at the Internet Governance Forum in Athens, as well as a researcher in e-commerce and Internet security issues. For more than for years, Violeta has worked in the ICT business sector in Macedonia, and now is a marketing consultant for a company specialising in ICT solutions and information security.

List of Discussion Papers:

1. The Network Neutrality Debate and Development
3. A study of the UN Working Group on Internet Governance
4. World Summit on Information Society and Develpment of Internet Diplomacy

This project has been made possible with support from

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA
Swiss Agency for Development and Cooperation SDC