I-WAYS, Digest of Electronic Commerce Policy and Regulation 26 (2003) 3–7
IOS Press

In Brief

Policy Frameworks for the Knowledge Economy

The capacity of countries, firms and industries to develop and manage knowledge assets is a major determinant of competitiveness and economic growth. It is on this important reality that the OECD (www.oecd.org) has an ongoing research program and recently sponsored the Global Forum on the Knowledge Economy, Policy Frameworks, ICTs, Innovation and Human Resources in Brasilia in September 2002. This Forum was organized in cooperation with the Ministry of Science and Technology of Brazil, the Inter-American Development Bank and *info*Dev. The general objectives of the Global Forum were (1) to stress the importance of a comprehensive policy framework that integrates ICTs, innovation and human resources; and (2) share experiences on the development and future directions of policy frameworks for the knowledge-based economy, and advance this general policy agenda.

The Forum provided an overview of policy developments reflecting an increased role of knowledge and management. Specific attention was given to three inter-related policy clusters: (1) Information technologies including communications infrastructure and e-business; (2) Science, technology and innovation, and; (3) Skills, education and knowledge-based employment. It was composed of five main sessions: (1) Economic Growth and the Knowledge-Based Economy; (2) Policies and Government Action for ICTs and E-Business; (3) Innovation; (4) Human Resources; and (5) Policy Roundtable. Topics for discussion included:

- What is the applicability of knowledge-based development strategies for Latin America and other emerging economies? What strategies best foster creative knowledge-based industries and activities?
- How can these strategies be broadly based to ensure that the whole economy contributes to and benefits from the growth of knowledge-based industries and activities?
- What kinds of strategies and economic conditions are promoting competitiveness along firm and industry value chains?
- What kinds of strategies encourage the growth of domestic high-value activities while maintaining and expanding openness to international networks?
- Are there new strategies to link FDI and foreign knowledge-based activities to domestic innovation and entrepreneurship?
- What are the strengths and weaknesses, opportunities and threats for developing knowledge-based activities in the current Latin American economic circumstances of slower growth and external capital market constraints?
- What are the priorities and sequencing for public and private sectors to continue building sustainable knowledge-based activities?

Speakers for the Forum were drawn from OECD, Latin American countries, the government sector and regulatory agencies, the private sector, civil society, and academia. An issues paper was prepared to provide a useful context for the event. Further information may be obtained from Mr. Graham Vickery (graham.vickery@oecd.org).

Homeland Security Seeks Advanced IT E-Solutions

The US Department of Homeland Security that began operations in January has a budget of US $38 billion. It consolidates 22 agencies employing a total of 170,000 federal employees – including the Federal Bureau of Investigation and the Central Intelligence Agency – under a single virtual roof. Its objective is to improve information sharing among agencies, secure the nation's mission-critical IT systems and eliminate redundancies in federal IT functions.

This has opened enormous opportunities for companies to aid the DHS in building and refining its inter-

ISSN 1084-4678/03/$8.00

nal IT infrastructure, and to contribute technologies to the department's overall effort to improve national and Internet security. Specifically, President Bush's 2003 budget has earmarked $722 million for initiatives to share information and intelligence across federal departments and among federal, state and local governments. It is estimated that nearly 5 percent of the department's $38 billion 2003 budget will be allocated to external spending on hardware, software and IT services.

DHS chief information officer Steve Cooper estimates that his office has already spoken to more than 1,000 companies about leading-edge technology that had not yet been commercialized and that could be used to further the DHS's mission.

At present, only a handful of IT organizations have won major contracts directly with DHS, largely because a portion of the department's budget for new IT infrastructure spending is frozen until it finalizes its enterprise architectural plan. However, additional major contracts have been inked with various agencies within DHS.

For example, UK-based *Autonomy* won a contract in October with DHS to provide software that analyzes multi-source information. Using natural language to help investigators better describe what they are tracking, the system can locate patterns and clusters of words. The application will enable government officials to monitor suspected terrorist groups and create a consolidated terrorist watch list.

Also, *Unisys* announced in September that it had won a $1 billion contract with the Transportation Security Administration, a part of DHS, to develop an IT and telecommunications infrastructure for 429 domestic airports and more than 180 other locations. The TSA effort aims to secure transportation systems throughout the United States. *Computer Sciences Corporation* (CSC) was subcontracted by *Unisys* for $50 million of the contract, which eventually will include securing railways, highways, transit systems, maritime operations and pipelines.

Unisys also garnered a $1.23 million biometrics research and development support contract with the Department of Defense in October. That contract calls for the company to develop a three-dimensional identification program that will help authorities better match images already on file for visa and passport applications and access controls. To aid in that effort, the company tapped *AcSys Biometrics*; researchers at the University of California at San Diego and Columbia University; *Identix*; *Genex Technologies*; and *Geometrix*.

Drawing up the service contract for the DHS is one of the department's next major hurdles, and leading vendors are jockeying for prime position. Smaller organizations stand a greater chance of making a deal if they partner with larger firms. Such companies as *SAIC, EDS, CSC, Northrop Grumman* and *Lockheed Martin* are in the strongest position to win homeland security federal contracts, according to IDC program manager Jocelyn Young. "They are the ones that have a broad portfolio of capabilities and services and a broad mix of partners that they can work with to meet the homeland security need," she said.

Young expects the department will sign contracts in two phases. Within the first year, the focus likely will be on setting up an internal IT infrastructure, including e-mail, secure collaboration technologies, such as Web and videoconferencing, and decision support applications. After that, Young anticipates that the DHS will focus on three key areas: biometrics, such as fingerprint scanning and fraud protections; data mining; and Geographic Information Systems, or GIS.

The challenge for the DHS is that a lot of the technologies they need is in startups, and emerging technologies are in the small to mid-sized firms. At least one program, started in 1999, could help. *In-Q-Tel*, a CIA-funded venture capital company, searches for technologies produced by startups, universities and established companies that could aid in intelligence gathering. Although *In-Q-Tel* may not be the complete answer to the government's needs, "it is a model for us to look at and ask how might we do this, and how might we encourage VCs to invest in technologies that would improve homeland security," said the Gartner analysts.

The 2003 budget also includes $12 million for pilot projects and $8 million to complete a national enterprise architecture. In 2004, the total allocation for those two program areas will increase to $28 million.

Council of Europe Recommends Freedom of Internet Communications

A Declaration on Freedom of Communications is being drafted by the Council of Europe (CoE), established to protect human rights in Europe. The Declaration is the latest initiative to address protection of individual rights in "information societies". A first draft was

made available on its website (www.coe.int) for public comment in April 2002 a revised and updated text was published in late November 2002. More than 40 countries are members of the CoE including all members of the European Union and 16 countries from central and eastern Europe. The need for this Declaration, according to the draft declaration, is to respond to "a marked tendency by some governments to restrict and control access to the Internet in a manner which is incompatible with international norms on freedom expression and information". The objectives of the declaration are to address "the removal of barriers to the participation of individuals in the information society, the freedom to provide services via the Internet, the liability of intermediaries, as well as anonymity".

The following is a summary of the principles contained in the Declaration:

Principle 1 – Content Rules for the Internet

This principle stresses that member States should not apply prohibitions to Internet content which go further than those applied to other more traditional media; content which is legal off-line should also be legal on-line.

This principle was advocated in a joint statement of the UN Special Rapporteur on freedom of opinion and expression, the OSCE Representative on freedom of the media and the OAS Special Rapporteur on freedom of expression, dated 22 November 2001.

Principle 2 – Self-Regulation or Co-Regulation

As already underlined in Recommendation Rec (2001) 8, member States should favor self-regulation or co-regulation regarding content disseminated on the Internet rather than regulation by the State. The need for setting up specific Internet regulatory bodies has not been demonstrated. However, it could happen that some member States decide to set up such bodies, or entrust an existing regulatory body with the legal competence to regulate Internet content. In this event, such bodies would have to meet the requirements of Recommendation Rec (2000) 23 on the independence and functions of regulatory authorities for the broadcasting sector, in particular with regard to their independence from political and economic powers and the possibility to subject their decisions to judicial review.

Since such regulatory bodies would deal with issues affecting freedom of expression and information, it is necessary to recall that they should also respect Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms.

Principle 3 – Absence of Prior State Control

This principle underlines the importance of no prior state control over what the public can search for on the Internet. In some countries, there is a tendency to block access by the population to content on certain foreign or domestic web sites for political reasons. This and similar practices of prior State control should be strongly condemned.

Although the State should by no means take broad measures to block undesirable content, exceptions must be allowed for the protection of minors. Where minors have access to the Internet, for example in schools or libraries, public authorities may require filters to be installed on computers to block access to harmful content.

The absence of prior control by the State does not of course rule out measures being undertaken to remove content from the Internet or block access to it following a preliminary or final decision of the competent national authorities on its illegality, not only under penal law, but also under other branches of law such as civil or administrative law. This would typically be the case when injunctions are sought to prevent the publication on the Internet of content which is illegal. Such measures, which could entail some sort of prior control, would have to fulfill the requirements of Article 10, paragraph 2, of the Convention for the Protection of Human Rights and Fundamental Freedoms and they would have to be directed at a clearly identifiable Internet content.

Principle 4 – Removal of Barriers to the Participation of Individuals in the Information Society

This part of the Declaration builds on principles already established in Recommendation No. R (99) 14 on universal community service concerning new communication and information services. It is stressed that member States should foster and encourage access for all to Internet communications and information services on a non-discriminatory basis, at an affordable price. In this Declaration, "access for all" is taken to mean access via public access points. Member States may of course go further, if they so wish, by encouraging individual access.

An active participation of the public in the information society, such as setting-up and running individual web sites, should also be encouraged. This means in practice that public authorities should not issue regulations which complicate the setting-up and running of

individual web sites, for example licensing or registration systems or any other requirements having a similar effect. A requirement, for instance, to notify the authorities of any changes to a web site might violate this part of the principle.

Principle 5 – Freedom to Provide Services via the Internet

While Principle 4 deals with access by private persons, Principle 5 focuses on the situation of service providers.

The aim of this principle is to underline that the provision of services via the Internet should not be subject to prior authorization by the State on the sole ground that this service is provided through the Internet. This is without prejudice to authorization schemes which govern the provision of services regardless of the means of delivery used (for example, regarding access to certain regulated professions), since these procedures do not address specifically and exclusively the Internet.

This principle is based on Article 4 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (hereinafter referred to as the "Directive on electronic commerce").

Principle 6 – Limited Liability of Intermediaries for Internet Content

Here it is established that as a general rule intermediaries in the communication chain should not be held liable for content transmitted through their services, except in certain limited circumstances. Along the lines of Articles 12–15 of the Directive on electronic commerce, the exemptions to liability take into account the different types of activities of the intermediaries, namely providing access to communication networks, transmitting data and hosting information. The degree of liability depends on the possibilities of service providers to control the content and whether they are aware of its illegal nature. The limitations on liability do not apply if intermediaries intentionally disseminate illegal content.

1st Paragraph – No General Obligation to Monitor

This paragraph is based on Article 15 of the Directive on electronic commerce. Member States should not impose any general obligation on service providers to monitor the information on the Internet to which they give access, that they transmit or store. Nor should they be subject to a general obligation to actively seek facts or circumstances indicating illegal activity, since this might have the effect of curbing freedom of expression.

This paragraph of Principle 6 does not prevent public authorities in member States from obliging service providers in certain cases, for example during a criminal investigation, to monitor the activities of their clients.

2nd Paragraph – "Mere Conduit"

In the case of mere transmission of information or providing access to communication networks, intermediaries should not be held liable for illegal content. When the role of intermediaries goes beyond that, in particular when they initiate the transmission, select the receiver of the transmission or select or modify the information transmitted, their liability may be invoked.

The activity of the intermediary which is at stake here, and which should be exempt from liability, is sometimes referred to as "mere conduit" (cf. Article 12 of the Directive on electronic commerce).

3rd Paragraph – "Hosting"

In the case of hosting content emanating from third parties, intermediaries should in general not be held liable (cf. Article 14 of the Directive on electronic commerce). This does not apply, however, when the third party is acting under the control of the intermediary, for example when a newspaper company has its own server to host content produced by its journalists. However, if the host becomes aware of the illegal nature of the content on its servers or, in the event of a claim for damages, of facts revealing an illegal activity, it may reasonably be held liable. The precise conditions should be laid down in national law.

4th Paragraph – "Notice And Take Down" Procedures and Freedom of Expression and Information

As stipulated in paragraph 3 of Principle 6 of the Declaration, service providers may be held liable if they do not act expeditiously to remove or disable access to information or services when they become aware, as defined by national law, of their illegal nature. It is to be expected that member States will define in more detail what level of knowledge is required of service

providers before they become liable. In this respect, so-called "notice and take down" procedures are very important. Member States should, however, exercise caution imposing liability on service providers for not reacting to such a notice. Questions about whether certain material is illegal are often complicated and best dealt with by the courts. If service providers act too quickly to remove content after a complaint is received, this might be dangerous from the point of view of freedom of expression and information. Perfectly legitimate content might thus be suppressed out of fear of legal liability.

5th Paragraph – The Possibility of Issuing Injunctions Remains Intact

It is highlighted here, in line with Articles 12–14 of the Directive on electronic commerce, that despite the above-mentioned limitations of liability, the possibility of issuing injunctions where service providers are required to terminate or prevent, to the extent possible, an infringement of law, remains intact.

Principle 7 – Anonymity

The aim of this principle is first and foremost to underline that the will of users to remain anonymous should be respected. There are two aspects to this principle. Firstly, users may have a valid reason not to reveal their identity when they have statements published on the Internet. Obliging them to do so could restrict excessively their freedom of expression. It would also deprive society of potentially valuable information and ideas.

Secondly, users need protection against unwarranted on-line surveillance by public or private entities. Member States should therefore, for example, allow the use of anonymity tools or software which enable users to protect themselves.

This principle has, however, its limitations. Member States should have the possibility of obtaining information about persons responsible for illegal activities within the limits laid down under national law, the Convention for the Protection of Human Rights and Fundamental Freedoms, in particular Article 8, and other relevant international treaties such as the Convention on Cybercrime.