I-WAYS, Digest of Electronic Commerce Policy and Regulation 27 (2004) 57–63
IOS Press


# In Brief

## Europe's Information Society Action Plan Advances

eEurope 2005, endorsed by the Council of Ministers in 2003, aims to develop modern public services and a dynamic environment for e-business through widespread availability of broadband access at competitive prices and a secure information infrastructure. The eEurope website contains extensive details on programs: http://www.europa.eu.int/information_society/eeurope/2005/index_en.htm.

The Information Society will affect most aspects of our lives, so policies are as diverse as the regulation of the sector to the protection of privacy.

For the purpose of this review the policies are grouped as follows: Regulating, Stimulating and Exploiting the Benefits of the Information Society, which includes issues such as protecting privacy and ensuring health and safety.

All these policies are, of course, heavily interrelated – as people and business exploit the benefits, for example, they generate demand, in turn stimulating further growth. Many policies therefore cross these boundaries, and so appear below more than once.

One policy initiative that crosses all of them, finally, is the eEurope 2005 Action Plan, a sort of high-level 'policy accelerator' that focuses attention on and pushes forward progress in seven '**eEurope policy priorities**': Broadband, eBusiness, eGovernment, eHealth, eInclusion, eLearning and Security.

The principle guiding eEurope is to stimulate demand and lower obstacles in parallel, getting around the 'chicken and egg' problems which often block the development of new products and services. Each eEurope priority therefore stimulates the development of a number of specific policies. It is complemented by eEurope+, launched by EU Candidate Countries in 2001.

*Regulating the Information Society*

The European Information Society sector has grown partly due to European initiatives such as the creation of the Single Market, the adoption of harmonized standards such as GSM, and the liberalization of the telecommunications sector. Today, a new electronic communications regulatory framework, launched in July 2003, provides a world-class legal framework for continuing the development of the industry, stimulating competition, creating growth and safeguarding public and user interests.

The new Framework covers, among other things, the management of scarce resources essential to communications. One particularly important resource is radio spectrum, through which all wireless communications travel, so the EU's new radio spectrum policy was launched as part of the new framework. However, while the Framework focuses on communications networks and services, radio spectrum policy covers *all* areas where spectrum is an issue, from mobile telephony to television broadcasting, from satellite positioning systems to scientific research, and much more.

These regulatory areas are also coordinated with the Radio Equipment and Telecommunications Terminal Equipment (RTTE) Directive, which regulates the telecommunications equipment market. By replacing over 1000 national approval regulations, the Directive has created a framework for regulating what is now a European single market worth 30 billion euro.

*Stimulating the Sector*

Policies here range from helping European industry develop new products and technologies to stimulate the appearance of new services and eBusiness.

eEurope 2005 policy priorities stimulate the sector by:

- promoting the development of the underlying infrastructure: (Broadband and Security)
- stimulating the supply of advanced services, notably via the public sector: (eGovernment, eHealth and eLearning)

ISSN 1084-4678/04/$17.00 

– promoting the uptake of eBusiness, building on policies such as the .eu domain, a key element in translating the European Single Market into the worlds of eBusiness.

*Research and Industrial Policy*

These priorities are complemented by the EU's drive to both underpin European industrial competitiveness through research and technological innovation (RTD) and to ensure that research supports other EU policies.

With most research in Europe fragmented into national programs, the Information Society Technologies priority within the EU's Sixth Research Framework Program focuses on bringing together universities, research institutes, small and large companies, governmental organizations and more across Europe to create the critical mass required to compete internationally.

The relevant EU Industrial policy promotes the competitiveness of the industries and services and supports the take-up of information and communication technology and e-business practices by European enterprises. Overcoming Obstacles to 3G Deployment, moreover, traces the development of European policy towards third generation ("3G") mobile communications in particular.

*Content and Services*

Stimulating the sector is also a question of stimulating the content and services which make the Information Society valuable. The public sector is the single biggest producer of information in Europe, producing data on topics as diverse as economics, traffic flow and demographics. The EU's Public Sector Information Directive therefore stimulates the sector by making it easier for companies to access and add value to this valuable raw material.

Europe's cultural heritage is another potentially massive source of content. Digitizing it would both stimulate the development of the Information Society and make this unique cultural heritage available to more people.

*Exploiting the Benefits of the Information Society*

A range of policies also aim to ensure that Europe exploits the possibilities offered by the Information Society.

Again, the eEurope 2005 emphasis on eGovernment, eHealth, eInclusion and eLearning aims to improve the lives of all Europeans through more effective, efficient and accessible public services. The eEurope goals of creating a dynamic eBusiness environment, underpinned by Secure and Broadband access, will stimulate European competitiveness and economic growth. The Information Society can also improve road safety.

Exploiting benefits can also mean ensuring that the Information Society does not have any negative effects, which requires policies:

– **protecting people's privacy** in the Information Society and **banning spam**: *Directive on Privacy and Electronic Communications*, part of the new communications regulatory framework;
– ensuring **e-Inclusion**;
– Ensuring that the new medium is Secure, and defining and fighting cybercrime;
– **dealing with illegal and harmful Internet content**: *Safer Internet Program*, which implements the *Recommendation on the Protection of Minors and Human Dignity* in online media;
– helping ensure the Quality of Health-related websites.

# Protection of Critical Information Infrastructure Requires New Legal Frameworks

Requirements for new laws and administrative activity under the rubric of homeland security "have kept the legal framework for critical infrastructure protection a moving target," so concludes a report prepared by the US National Research Council (NRC). A new report, *Critical Information Infrastructure Protection and the Law: An Overview of Key Issues*, pointed out that all critical infrastructures are increasingly dependent on the information infrastructure for information management, communications and control functions. To help better address these challenges, the NRC prepared this report to assess the various legal issues associated with Critical Information Infrastructure Protection (CIIP). These issues include incentives and disincentives for information sharing between the public and private sectors, and the role of the Freedom of Information Act (FOIA) and antitrust laws as a barrier or facilitator to

progress. The report also provides a preliminary analysis of the role of criminal and liability laws, and the establishment of best practices, in encouraging various stakeholders to secure their computer systems and networks.

The report examines the range of legal issues associated with information infrastructure protection, particularly those that affect the willingness of private sector companies and organizations to cooperate with the government to prevent, detect, and mitigate cyber-attacks. It separately considers different aspects of information sharing and liability – recognizing that there is a tension between these approaches that strategies for critical information infrastructure must ultimately resolve.

In a chapter titled The Big Picture, the report stresses the legal framework for CIIP must be considered in the larger context of the business, social and technical environment. "The increasing dependence on common technology and interconnected systems suggest that many of the technical vulnerabilities can be overcome only through collective, concerted action. Externalities are common in computer network security; the incentive that one network owner has to invest in security measures is reduced if the owner believes that other connected networks are insecure. Insurance can play a role in motivating the private sector by transferring the risk of computer security losses from a company to the insurance carrier. The few cyber insurance policies in effect today require companies to employ appropriate security measures. Most policies also require firms to undergo an initial independent security evaluation of network defenses and ongoing intrusion-detection tests during the life of the policy.

Prior to September 11, the security of information systems and the protection of personal data and privacy were considered to be mutually reinforcing and compatible goals. Many experts suggest that the crisis-management mentality in the aftermath of September 11 has pushed aside issues of privacy and civil liberties. Technical mechanisms proposed to aid government efforts in the war on terrorism appear, to some, to sacrifice privacy and civil liberties for only the illusion of an increased ability to protect the nation's infrastructures. Mechanisms should be implemented to ensure that surveillance conducted to combat terrorists and hackers does not result in a loss of privacy for innocent citizens.

Trust among those sharing information is one of the most important prerequisites for successfully protecting the nation's critical information infrastructures. Trust is necessary to achieve an atmosphere of openness and cooperation. Although trust has been a central component of the government's CIIP efforts over the past several years, the government has failed to build sufficient trust between the public sector and the private sector for four reasons. First, the government's message to the private sector has vacillated – at times it stresses national security, at other times economic viability – raising concerns about whether the priority of the day will trump prior promises. Second, the government has so many focal points for CIIP that firms often do not know which agency to contact or what authority and established processes underpin the promises of that agency to protect information from disclosure. Third, the government has been slow to reciprocate in sharing information with the private sector. Finally, in the aftermath of September 11, the government took actions that produce a perception (right or wrong) that it may unilaterally suspend prior agreements with respect to the nondisclosure of information if it deems that circumstances warrant."

*The final report "Critical Information Infrastructure Protection and the Law: An Overview of Key Issues," is a publication of the National Academies press in 2003 and is available for purchase or online reading at http://books.nap.edu/catalog/10685.html.*

# E-commerce Trade Rules Delayed in WTO, Adopted by FTAs

At the last meeting of the WTO Work Program on Electronic Commerce in October 2002, there were two items on the agenda: (1) classification of the content of certain electronic transmissions, and (2) fiscal implications of E-Commerce. Classification had been an issue in previous E-Commerce discussions, the essential question was "whether digital products were goods or services, or in fact they could be either." Several members pointed out that services might be involved in the delivery of a product, such as the downloading of software, but did this make the product a service? For example, an automobile was not considered a service simply because design services, computer aided related services, and distribution services were involved in its production. The key issue, it was widely agreed, was that producers and exporters of digital software products want to ensure the most efficient method of de-

livering their products. Rules for electronic products should be no more restrictive than if the product were delivered physically. The current liberal trading system should be maintained.

Another more simplified view was recommended for approval – products delivered in a physical form fall under the GATT and those delivered electronically fall under the GATS. At the conclusion of the meeting there was no consensus on classification meaning that E-Commerce continues to be an unresolved new trade issue. The impasse in the WTO may have been overtaken by the decision by a number of governments and regional organizations to negotiate free trade agreements (FTAs) with a strong focus on services, with telecommunications and E-Commerce included in most of these agreements. The classification issue is essentially resolved in these agreements.

The United States has initiated a number of bilateral FTAs and several regional FTAs. In the FTAs between the US and Australia, Chile, Singapore, Jordan, Morocco and Central America, a template or model E-Commerce text has been included. The full texts of US FTAs are available on the website of the US Trade Representative: www.ustr.gov. The E-Commerce chapter of these agreements are linked to other chapters that may have a bearing on aspects of trade in services. Electronic supply of services are defined as the supply of a service employing computer processing thus falling within the scope and obligations contained in articles on Cross-Border Trade in Services, Investment and Financial Services and subject to those relating to Non-Conforming Measures. Several standard provisions appear in each agreement:

Customs Duties: A Party shall not impose customs or other duties, fees or charges on or in connection with the importation of exportation of digital products, regardless of whether they are on a fixed carrier medium or transmitted electronically. However, this does not preclude a party from imposing internal taxes or other internal charges on digital products provided that such taxes or charges are imposed in a manner consistent with this Agreement.

Non-Discriminatory Treatment of Digital Products: A Party shall not accord less favorable treatment to some digital products than it accords to other digital products: (a) on the basis that the digital products receiving less favorable treatment are created, produced, published, stored, transmitted, contracted for, commissioned or first made available on commercial terms outside its territory; or (b) on the basis that the author, performer, producer, developer of distributor of such digital products is a person of the other Party or a non-Party; or (c) so as to otherwise afford protection to other like digital products that are created, produced, published, stored, transmitted, contracted for, commissioned or first made available on commercial terms on its territory.

The previous paragraphs do not apply if non-conforming measures are adopted or are inconsistent with provisions of the agreement relating to Intellectual Property rights, where subsidies or grants provided to a service or service supplier by a Party, including government-supported loans, guarantees, and insurance, and services supplied in the exercise of governmental authority within the territory or each respective Party. A Party is not prevented from adopting or maintaining measures in the audio-visual and broadcast sectors, in accordance with other Chapters in this Agreement. Nothing in this article shall be construed as affecting the application of Article 4 of the TRIPS Agreement.

Authentication and Digital Certificates: Each Party shall maintain domestic legislation for electronic authentication that: (a) permits parties to an electronic transaction to determine the appropriate authentication solutions and implementation models for their electronic transactions, without limiting the recognition of technologies and implementation models; and (b) permits such parties to have the opportunity to prove in court that their electronic transmission complies with any legal requirements with respect to authentication. That is, a Party is required to create or maintain an authentication regime for electronic transmissions.

Other Consumer Protection: The Parties recognize that consumers who participate in electronic commerce should be afforded transparent and effective consumer protection under their respective laws.

Paperless Trading: Each Party shall endeavor to make available to the public, in electronic form, all existing trade administration documents, and shall endeavors to accept trade administration documents transmitted electronically as the legal equivalent of paper documents.

Definitions: For the purposes of this Chapter:

*Carrier medium* means any physical object capable of storing a digital product, by any method now known or later developed, and from which a digital product can be perceived, reproduced, or communicated, directly or indirectly, and includes optical medium, floppy disk and magnetic tape;

*Digital product* means the digitized form or encoding of, computer programs, text, video, images, sound

recordings, and other products, regardless of whether they are fixed on a carrier medium or transmitted electronically; digital products can be a component of a good, to be used in the supply of a service, or exist separately, but do not include the digital representations of financial instruments that are settled or transmitted through a central bank-sponsored payment or settlement system;

*Electronic transmission or transmitted electronically* means the transfer of digital products using any electromagnetic or photonic means; and

*Trade administration documents* means forms issued or controlled by a Party which must be completed by or for an importer or exporter in relation to the import or export of goods.

# Disappointing Use of ICT in High Schools – OECD Report

Major investment outlays over the past 20 years have brought ICT into nearly all schools in the most advanced OECD countries, but the extent to which computers are in day-to-day use in these schools remains disappointing, according to the OECD report *Completing the foundation for lifelong learning: An OECD survey of Upper Secondary Schools*. The report draws on data from 14 OECD countries – Belgium (Flanders), Denmark, Finland, France, Hungary, Ireland, Italy, Korea, Mexico, Norway, Portugal, Spain, Sweden and Switzerland – to review the structural barriers preventing full and effective use of ICT in upper secondary schools. Its conclusions raise important issues for the scheduling of teachers' time, classroom organization and teachers' professional development.

Despite the large sums of money spent on ICT, fewer than 20 per cent of students attend schools where there are enough workstations for every teacher to have one, according to this OECD report. And in 11 out of 14 countries surveyed, a shortage of computers for students was cited as one of the biggest obstacles to greater ICT use. Educational use of computers is in fact sporadic across all countries, with information gathering from the Internet being the most common way in which computers are used. On average across the countries surveyed, the principals of only around 20 per cent of students reported that computers are used a lot as a source of additional instruction or to allow students to work at their own pace. Only a minority of teachers across countries regularly use standard computer applications, according to their principals, and only in Denmark, Sweden and Korea do the proportions who do so reach 60 per cent.

Given the explosion in use of ICT in other walks of life, these figures are surprisingly low. The most common reasons cited for this under-use are: difficulties in integrating ICT into classroom instruction; problems in scheduling enough computer time for classes; and teachers' lack of ICT skills and knowledge. In addition, principals report that recruiting ICT teachers is by far the most difficult recruitment problem that they face across all school subjects. Other key findings in the report are:

The extent of selection in admission and grouping policies varies greatly between countries. Belgium's Flanders region and Hungary are on average more selective, while Norway and Sweden are at the other end of the spectrum. However, the study also suggests that selective policies do not always lead to less equitable outcomes.

The guidance and support which students receive plays a part in this. Particularly well developed career guidance systems are to be found in Denmark, Finland, Korea and Ireland, where more than 80 per cent of students receive individual career counseling in the last year of their upper secondary programs.

Seeking feedback from stakeholders and others is indicative of an adaptive organization responding to the world which it must prepare its students for. The survey results suggest that on average Finland, Hungary and Korea receive feedback from the greatest range of stakeholders.

All countries face some difficulties in hiring teachers and there is significant variation within countries. In Belgium's Flanders region, the majority of students attend schools where principals report above average difficulties in hiring teachers. Above average difficulties are also reported for Finland, Ireland and Switzerland. These countries succeed to varying degrees in filling vacant posts with fully-qualified staff. In both Flanders and Ireland, 95 per cent or more of pupils attend schools that fill vacancies with fully qualified staff.

Assessing countries across these and other benchmarks derived from the study, indicates that all countries have strengths and weaknesses within their upper secondary school systems. Overall, the Nordic countries – Denmark, Finland, Norway and Sweden appear

to have the greatest number of strengths, followed by Korea. For the Nordic countries much of this strength is centered on the availability and use of computers and teachers professional development. The challenges which countries generally face in these areas have to be tackled also by the Nordic countries though these findings suggest that they may have something of a head-start with this.

The report is available at www.oecd.org.

# Bush Promises Universal Access to Broadband in the US by 2007

Included in new technology initiatives announced in April by President George W. Bush are proposals to "wire America with fast Internet connections." Bush's goal is for "every corner of the United States to be in reach of high-speed Internet links by 2007." Broadband connectivity, Bush stressed, "guarantees that we have access to the information that is transforming our economy." Federal agencies were ordered to streamline the process of granting broadband service providers access to federal land. The Administration is supporting FCC efforts to deregulate fiber-optic connections, as well as the Department of Commerce's development of specifications for broadband over power lines.

In an effort to spur investment, the President signed into law a jobs and growth package that allowed companies to depreciate capital expenditures more quickly, including capital equipment used for broadband deployment. Companies are more likely to make important investments in broadband technology if they can depreciate the capital costs associated with rollout more quickly.

The President has signed into law into law a two-year extension of the Internet Access Tax moratorium and has called on Congress to pass legislation that would explicit extend the moratorium to broadband and make the moratorium permanent. Taxing broadband access would increase the cost of broadband for consumers.

The Administration supports the Federal Communications Commission (FCC) decision to free new fiber-to-the-home investments from long-time regulations. Deregulating new ultra-fast broadband infrastructure to the home removes a significant barrier to new capital investments.

The Administration has made unprecedented strides in balancing the commercial spectrum needs of critical government agencies (including Departments of Defense, Transportation and Homeland Security) and commercial interests. It has identified 90 MHz of spectrum to be auctioned for next generation services. Currently only one wireless carrier is offering wireless broadband. Once the 90 MHz is auctioned, multiple wireless carriers will have the opportunity to become broadband carriers – stimulating vigorous competition and bringing lower prices and improves services to consumers.

In addition to the broadband initiative, Bush called for a government program to create national standards that would enable medical information to be digitized, stored and shared electronically. "Within 10 years every American must have a personal electronic medical record," Bush said. He emphasized the federal government must take the lead in order to make this happen. The plan announced by the White House indicates it will include "electronic prescriptions" that can be sent to pharmacists and supplant handwritten ones. Federal programs such as Medicare, Medicaid and Veterans health care are to move toward electronic record-keeping. Privacy and security guidelines would be incorporated into those standards.

*The full text is available at http://www.whitehouse.gov/infocus/technology/*

# India Plans Data Protection Legislation

There is growing pressure on the Government of India to adopt a national data privacy law that would be equivalent to the protection provided by European Data Protection legislation. This is a message strongly presented by the European Commissioner for Information Society Erkki Liikanen at a conference in New Delhi in March. Rapid growth in India of outsourcing services from US and European companies, involving processing customer data and call centers that handle personal information is raising concerns over the absence of a law for the equivalent protection of such data. According to the European Union, its Data Protection Directive requires "equivalent treatment of data" about Europeans or export can be denied.

Indian authorities report this is largely an outsourcing issue because within India, only a limited num-

ber of companies are computerized sufficiently to process personal records. However, following elections in April, it is understood a project will be launched by the Ministry of Information Technology to draft legislation. Moreover, some groups in India have indicated they will welcome recognition of personal information rights by the government.

The European Commission and US companies for many years have held divergent views on how formal instruments to protect personal data transferred across the Atlantic should be. The EU has been seeking comparable public law but the US negotiated a "Safe Harbor" agreement whereby American companies make a written commitment to the US Department of Commerce pledging they have adopted and enforce protective measures for name-linked data holdings. Some American companies are said to believe that if Indian companies sign letters promising to protect all personal data in their possession, this will be satisfactory. However, a bill recently introduced in the US Senate by Senator Hillary Clinton would "prohibit the communication of personal information about US citizens to any foreign country that has failed to adopt an 'adequate' privacy regime."

If India should put forward a proposal to the Europeans to establish a "Safe Harbor" agreement similar to the text with the US, rather than its parliament adopting legislation containing enforcement powers and possibly a data protection authority, the European Commission would face a dilemma. Officials in Brussels have suggested the Commission will adopt a rather strong view toward what may be proposed as "adequate protection" by developing countries. Because countries such as China, Thailand, Brazil, Pakistan and Indonesia have not adopted national privacy policies or laws and are increasingly engaged in outsourcing and cross-border services trade, it is likely the Commission will insist on formal legislation modeled after European statutes.