I-WAYS, Digest of Electronic Commerce Policy and Regulation 28 (2005) 3–7
IOS Press

In Brief

US Continues Ban on Internet Taxation

The US Congress on November 19, 2004 adopted the Internet Tax Non-Discrimination Act. The moratorium extends a ban on Internet taxation of three types: taxes on Internet access, double taxation by two or more states of a product or service purchased over the Internet; and discriminatory taxes that treat Internet purchases differently from other types of sales. The ban applies to all types of Internet technologies, including dial-up, DSL, cable modem and wireless service.

Congress first passed a temporary moratorium in 1998 restricting taxation of Internet access, which expired in November 2004. The new legislation will expire in three years. However, the legislation includes grandfather clauses for states that taxed Internet access in 1998 or are currently taxing high-speed wireline and wireless Internet access.

"For today's information based-economy, this legislation ensures that consumers will benefit from more competition, increased investment and new innovative services," said Walter McCormick Jr, president and CEO of the US Telecom Association. The legislation was strongly endorsed by American telecom providers and Internet service companies.

Safer Internet to be Promoted by EU Telecom Council

This four-year program proposed by the European Commission, called Safer Internet Plus, will have a budget of $60 million to combat illegal and harmful Web content. Its focus is on end users: parents, educators and children. In mid-December the EU Telecommunications Council met in Brussels to give political agreement to the European Commission's new multiyear program to promote safer use of the internet and new online technologies.

The Safer Internet Plus (2005–08) program will have a budget of Euro45m to combat illegal and harmful internet content. The new program also covers other media such as videos, and explicitly addresses the fight against racism, and also spam.

The program will bring in the new member states and focus more closely on end users: parents, educators and children. It also aims to mobilize talent in the public, private and voluntary sectors to prepare hard-hitting safety campaigns. The four action lines of Safer Internet Plus are fighting illegal content, tackling unwanted and harmful content, promoting a safer environment, and awareness-raising.

Safer Internet Plus is a follow-up to the existing Safer Internet Program, which has been in place since 1999. In October 2004, the EU's Dutch Presidency, in cooperation with the Commission, sent member states and stakeholders a questionnaire aimed at assessing progress in the EU on combating spam.

A workshop in Brussels on November 15 examined the results of this consultation, and highlighted both the need to adapt measures to address the changing nature of spam.

The Council recognizes the changing nature of spam, which is no longer just unsolicited commercial communications, but increasingly typified by viruses and other malicious code aimed at taking control of networks and single PCs, often for illegal activities. The origin of spam is also becoming more difficult to trace. The Council will look into national laws on privacy.

ISSN 1084-4678/05/$17.00

UK Reports Local Authorities E-Government Savings

The U.K. government has promised local authorities they stand to save some US$ 617 million a year by implementing its local e-Government national projects. On top of this significant savings, local governments in England, also called councils in the U.K., could increase total revenues by US$ 125 million per year, while delivering service improvements worth US$ 2.7 billion, the Office of the Deputy Prime Minister (ODPM) announced recently. Those figures are the average in a range for each category, according to a spokesman from the National Projects Program.

The ODPM is basing its claims on a study it commissioned from the French IT consulting and services specialist CapGemini SA, which looked at six of the 22 national projects the government is promoting as part of its push to deliver local e-Government by 2005. The six projects studied were: CRM (customer relationship management); workflow; local authority Web sites (called LAWs); mobile working (called NOMAD); online planning and regulatory services; and council tax and business rate valuation (Valuebill).

"These programs were chosen for study because they are a good sample for the program as a whole and because they are the most well developed of all the programs," said a spokesman from the National Projects Program.

The government has long pushed e-Government's benefits, though it has struggled to meet its own deadline of putting all government services online by 2005. Analysts have long warned that the government will be unable to reach its targets.

Last year, IDC published a report stating that the U.K. government was falling behind its European counterparts in providing its citizens with e-Government services. Forrester Research Inc. also published its own findings that the government would fail to reach the 2005 self-imposed deadline, partly because it doesn't understand how to work with fast moving, small e-Commerce vendors and how to build partnerships.

But the government continues to assert it is on the right track, though privately sources concede the 2005 deadline is now simply more of a guideline.

The ODPM set up the local e-Government National Projects Program to help all English local authorities achieve the 2005 local e-Government targets and develop a vision for e-Government within their own authorities. The funding comes from the ODPM, but the National Projects are run by local authorities for the benefit of other local authorities.

The National Projects Program spokesman said the government doesn't know exact numbers in terms of which councils adopted what programs, but said that 80 percent of councils "are already involved in at least one national project." The spokesman said that "involvement" went beyond simply inquiring about a program, but didn't necessarily include commitment to implement.

The 22 national projects also include a DigitalTV program that would enable councils to run an interactive digital TV channel to publish information and conduct polls.

Cybercrime Dramatic Growth in 2004

Cybercrime of all types grew exponentially in 2004, according to a BBC News report. This includes viruses that increased by more than 50%, phishing by 30%, as well as so-called bot-nets, used by hackers to carry out other different cyber crimes. Phishing is now considered a severe threat to E-Commerce customers who are tricked into divulging confidential personal financial data. The number of teenage hackers who are writing fast-spreading viruses, has rapidly grown in the last 12 months, according to experts. Young virus writers seem less inclined to use mass-mailing viruses, rather they are employing more surreptitious viruses or worms.

The Anti-Phishing Working Group has reported that the number of phishing attacks against new targets at a rate of 30% or more per month. The consequences for those impacted is usually emptying their bank accounts or identify theft that can cause long-term harm to reputations and employment.

Symantec security experts say worm writers are more interested in recruiting PCs to take part in "bot-nets" that can be used to send spam or to mount attacks on websites. The number of active "bot computers" rose from 2,000 to 30,000 per day last year, Symantec estimates. In the past many viruses had been the work of an individual or group, but today the code for viruses may be held by many groups that work on them to

produce new variants at the same time. It is estimated there may be more than 3,000 variations of the Spybot worm. Due to the co-existence of so many worms, it has become very difficult to understand chronology, Symantec concludes.

The emergence of the first proper virus for mobile phones occurred in 2004. In June, a virus was discovered that can hop from phone to phone which surreptitiously sends messages to premium rate numbers, and in November another virus emerged that can cripple phones.

US Business Calls for Tighter Cybersecurity Control

Security industry executives are calling on the Bush Administration to give greater attention to increasing cyber attacks that they conclude are threatening the country's critical network infrastructures. The Cyber Security Industry Alliance (CSIA), composed of executives of major security firms, urged the Administration to give a much higher profile within the administration. It has been two years since Bush proposed a National Strategy to Secure Cyberspace, involving a partnership between the public and private sectors to share security intelligence, reduce vulnerabilities and deter malicious entities.

The Administration's position is that cyber security's moving forward will inherently be part of any new federal government IT initiatives. Others, however, believe the President should create a distinct administrative cybersecurity position within the Homeland Security Department to oversee progress in the federal government and act as a liaison with private industry.

Cybersecurity costs are expected to be factored into all agency budget requests. It is a matter the Administration takes seriously enough that the Office of Management and Budget suggests agencies without adequate plans to improve cybersecurity shouldn't move to any new IT projects until cybersecurity is addressed, said Karen Evans, OMB's administrator for E-Government and IT.

Entering his second term, President Bush faces a number of challenges to IT-related initiatives such as cybersecurity. Perhaps the greatest challenge is a growing budget deficit projected to reach $521 billion for fiscal 2004. The president has promised to cut the deficit in half within five years, but much of this will depend on a reduction in spending, including a heavy reliance on IT to cut costs.

"This doesn't necessarily mean that IT budgets will be cut," Evans says. "If an agency is properly managing their portfolio, their IT budget might go down because they're achieving the same or better results with the same amount of tax dollars."

It is widely acknowledged the Department of Homeland Security has made some progress regarding cybersecurity, many experts would like to see responsibility for cybersecurity and physical security divided between two assistant secretaries. Robert Liscouski, Homeland Security assistant secretary for infrastructure protection, handles both. "We don't have that senior-level focal point to work with both industry and government on cybersecurity matters," he says.

When Congress in December adopted a simplified version of its Intelligence Reform Act after cutting a provision that would have created a high-profile assistant secretary of cybersecurity within Homeland Security, advocates perceived this as a slight to cybersecurity's importance. Evans says the formal creation of an assistant secretary for cybersecurity position is unnecessary. Any distinct cybersecurity position within Homeland Security is a management issue that should be worked out within the department, she says.

There is wide consensus that the nation's data and IT infrastructure will only be protected through a partnership of government and industry. Such a partnership includes calling on private-sector companies to secure their systems, but also government's willingness to apply successful private-sector cybersecurity initiatives to its own systems. Business leaders have called on the Commerce Department to urge CEOs across the US to review cybersecurity measures during board meeting reviews of business operations.

Setting aside the debate over the assistant secretary position, there is optimism cybersecurity will improve if the Senate ratifies the Council of Europe's Convention on Cybercrime and the Bush administration can encourage information-security governance in the private sector.

Global Trustmark Alliance Formed

The establishment of a global online consumer protection network has moved a major step closer as a result of a recent conference in Kuala Lumpur, Malaysia.

Self-regulatory organizations from eight nations in Asia, Europe and the Americas, an Asian coalition of e-commerce organizations, and three pan-European bodies, announced today the formation of an organizing committee that will establish a Global Trustmark Alliance (GTA). The new alliance intends to promote safe electronic commerce within each of the participating jurisdictions, and a trustworthy system for cross border e-commerce.

"This is an important development for the growth of e-commerce," Steven Cole, GTA's Executive Director and senior vice president of BBBOnLine, told the GBDe Summit today. "We all know consumer trust and confidence is crucial to growth, and this is even more important for trade across borders. International cooperation amongst key regional organizations that all help consumers find trustworthy online businesses promises to fuel interest in cross border e-commerce," Cole added.

The Asia Trustmark Alliance (ATA), one of the existing trustmark alliances at a regional level, and its members, will be part of the GTA pioneering committee. Dr Ho-Ming Huang, Chairman of ATA said that "after laying the foundation for a pan-Asian collaborative framework, it is only natural that Asia Trustmark Alliance looks toward closer co-operation at an international level." "In this respect, it is in the mutual interest of both trust organizations to work together to achieve our similar objectives, which is promotion of trustworthy e-commerce environment," Huang added.

The announcement was made at the 2004 summit of the Global Business Dialogue for Electronic Commerce (GBDe). The GBDe is a CEO-driven organization that has been instrumental in promoting international rules to promote worldwide growth in e-commerce. It has supported the formation of the GTA since it was first conceived and was instrumental in bringing diverse trustmark organizations together for the first time. The GTA is an outgrowth of recommendations made by GBDe in past years for close cooperation amongst trustmark programs and for the linking together of dispute settlement mechanisms.

The organizations participating in GTA are:

From the Americas:

- BBBOnLine (United States)
- BBBOnLine (Canada)

From Asia:

- Asia Trustmark Alliance
- Korea Institute for Electronic Commerce (Korea)
- National Trust Council, and its accredited trustmark programs, CommerceNet and Case Trust (Singapore)
- Secure Online Shopping Association (Taiwan)
- Electronic Commerce Promotion Council (Japan)

From Europe:

- Trust UK (United Kingdom)
- E-comtrust (European and Switzerland)
- Eurochambres (European)
- Federation of European Direct and Interactive Marketing (European)

Many of the participating organizations operate trustmark programs that allow businesses that meet high standards to display a trustmark, or label, on e-commerce web sites. All of the organizations promote self-regulatory codes of online business practices and effective dispute settlement procedures.

The GTA Organizing Committee will begin work immediately to share best practices in the administration of trustmark programs, and to establish cooperative procedures to resolve cross border complaints. GTA's longer term goal is to harmonize the various voluntary online business practice codes, and to issue an international GTA trustmark that would be co-branded with the local trustmarks used in each jurisdiction.

For details on trustmark organizations in a number of countries, refer to the GTA web site at www.globaltrustmarkalliance.org

Should Developing Countries Enforce Intellectual Property?

This research paper, To What Extent Should Less Developed Countries Enforce Intellectual Property, confronts many of the most debated issues involved in intellectual property protection by developing countries. It considers the consequences of IP enforcement in less developed countries (LDCs) for global innovation and

welfare in poorer countries. The potential merits of an industrial policy based on open source software also are discussed. The costs and benefits favoring IP enforcement for small, open developing countries are examined by Gilles Saint-Paul of the University of Toulouse, France in a publication of the AEI-Brookings Joint Center for Regulatory Studies.

The author addresses many of the most controversial aspects of the IP protection debate. The subject is introduced as: "Many advocates recommend that LDCs should not enforce intellectual property rights (IPRs). Their arguments have many facets. First, LDCs are "poor", and it would be unfair for them to pay high prices for patented goods. Second, historically, countries like the United States have not enforced IP, and seemingly have benefited from it. Third, some argue that LDC governments should promote non-IP options such as open source software, as an adequate strategy for development."

http://www.aei.brookings.org/admin/authorpdfs/page.php?id=1061

ITU Launches Multipurpose Community Telecenters in Africa

The International Telecommunication Union (ITU) is launching an initiative to establish a network of at least 100 Multipurpose Community Telecenters (MCTs) in 20 African countries. The MCTs will provide critical access for communities to Information and Communication Technologies (ICT), to help ensure these communities can obtain the social and economic benefits that come with participation in the Information Society.

The MCTs are to be managed by women, which will enable them to actively participate in the development and decision-making processes of the African continent. This initiative is in partial fulfillment of the commitment made by 175 countries to a Plan of Action at the first phase of the World Summit on the Information Society to extend the benefits of ICTs to all of humanity.

"Multipurpose Community Telecenters are one of the most innovative and practical ways to bring the benefits of the Information Society to the people of Africa. Not only will they create employment and provide basic information services but they establish community focal points for e-Education, e-Health and e-Governance initiatives through web-based multimedia content," says Mr. Hamadoun I. Touré, Director of the ITU Development Bureau. "They also stimulate the development and growth of local businesses as well as ICT skills among the local population."

The importance of this initiative for African women can't be understated, adds Ms. Asenath Mpatwa, the ITU Project Manager. "The MCTs provide an enabling environment where women can actively participate in the economy and expand their role in communities through the use of ICTs and the provision of new services."

Ms. Mpatwa noted that in addition to enhancing the development of sectors like education, health and agriculture, the initiative opens the door to partnerships with the private sector to assist in providing the necessary technology for the centers. "In exchange companies will get a better understanding of the potential of the ICT market in Africa and of women as active participants in its economy."

The initiative was requested by a number of African countries including Benin, Burundi, Central African Republic, Democratic Republic of Congo, the Gambia, Guinea Bissau, Kenya, Malawi, Congo, Rwanda, Tanzania, Zambia and Ethiopia. ITU, in cooperation with the African Ministries of Communication and other local partners, has established four MCTs in Tanzania and Guinea Bissau. These are now already providing basic training in the use of computers, and will soon supply other services such as public telephone, fax and internet connectivity as well as basic information.

International organizations and private sector suppliers of equipment and services are encouraged to contribute with expertise, specialized equipment and software.