I-WAYS, Digest of Electronic Commerce Policy and Regulation 27 (2004) 115–120
IOS Press

In Brief

Antigua and United States to Negotiate WTO Internet Gambling Ruling

The World Trade Organization Dispute Settlement Board (DSB) panel in early 2004 ruled in the Internet gambling dispute filed by Antigua and Barbuda against the United States that the US is in violation of WTO multilateral trade agreements. The case involves the US Wire Act that prohibits foreign and US persons from engaging in betting or wagering in US foreign or interstate commerce. Antigua contends the US is interfering with international commerce. In order to avoid the DSB issuing a final decision, a compromise may be negotiated by trade representatives of the two countries.

It has been reported that the US could offer Antigua a number of concessions to persuade the Caribbean country that its interests are best served by settlement, while at the same time preserving the US Government's interpretation of the Wire Act. Such a settlement might take the form of financial remuneration. Or, the US may choose to adjust Wire Act enforcement guidelines so as to reduce the risk that Antiguan Internet gambling companies would necessarily need to follow some "safe harbor" guidelines, such as not targeting the US market or US consumers, not advertising in the US, nor taking other actions to attempt to attract US customers.

Antigua may decide to postpone the negotiations for up to 12 months. This or other delays would push the negotiations past the US national elections, after which the Administration might have a freer hand to settle the dispute.

Government Surveillance Using Business Increases – Civil Liberties Group Complains

"The government is increasingly using corporations to do its surveillance work, allowing it to get around restrictions that protect the privacy and civil liberties of Americans," the American Civil Liberties Union (ACLU) claimed in a report issues in August 2004. ACLU works to protect civil liberties in the United States.

According to the ACLU, data aggregators–companies that aggregate information from numerous private and public databases–and private companies that collect information about their customers are increasingly giving or selling data to the government to augment its surveillance capabilities and help it track the activities of people.

Because laws that restrict government data collection don't apply to private industry, the government is able to bypass restrictions on domestic surveillance. The ACLU urged Congress to close such loopholes before the exchange of information grows out of hand.

"Americans would really be shocked to discover the extent of the practices that are now common in both industry and government," said the ACLU's officer Jay Stanley, author of the report. "Industry and government know that, so they have a strong incentive to not publicize a lot of what's going on."

Last year, JetBlue Airways acknowledged that it secretly gave defense contractor Torch Concepts 5 million passenger itineraries for a government project on passenger profiling without the consent of the passengers. The contractor augmented the data with passengers' Social Security numbers, income information and other personal data to test the feasibility of a screening system called CAPPS II. That project was slated to

ISSN 1084-4678/04/$17.00

launch later this year until the government scrapped it. Other airlines also contributed data to the project.

Information about the data-sharing project came to light only by accident. Critics like Stanley say there are many other government projects like this that are proceeding in secret. The ACLU released the Surveillance-Industrial Complex report in conjunction with a new website designed to educate the public about how information collected from them is being used.

The report listed three ways in which government agencies obtain data from the private sector: by purchasing the data, by obtaining a court order or simply by asking for it. Corporations freely share information with government agencies because they don't want to appear to be unpatriotic, they hope to obtain future lucrative Homeland Security contracts with the government or they fear increased government scrutiny of their business practices if they don't share.

Presently, the increasing amount of electronic data that is collected and stored, along with developments in software technology, make it easy for the government to sort through mounds of data quickly to profile individuals through their connections and activities. Although the Privacy Act of 1974 prohibits the government from keeping dossiers on Americans unless they are the specific target of an investigation, the government circumvents the legislation by piggybacking on private-sector data collection.

Corporations are not subject to congressional oversight or Freedom of Information Act requests–two methods for monitoring government activities and exposing abuses. And no laws prevent companies from voluntarily sharing most data with the government. "The government is increasingly. . . turning to private companies, which are not subject to the law, and buying or compelling the transfer of private data that it could not collect itself," the report states.

A government proposal for a national ID card, for example, was shot down by civil liberties groups and Congress for being too intrusive and prone to abuse. Congress voted to cancel funding for John Poindexter's Total Information Awareness, a national database that would have tracked citizens' private transactions such as Web surfing, bank deposits and withdrawals, doctor visits, travel itineraries and visa and passport applications. But according to ACLU contracts by the Justice Department's Drug Enforcement Administration and other federal authorities, continue to access billions of records on interests, lifestyles and activities of Americans.

By using corporations, the report said, the government can set up a system of "distributed surveillance" to create a bigger picture than it could create with its own limited resources and at the same time "insulate surveillance and information-handling practices from privacy laws or public scrutiny."

Every time people withdraw money from an ATM, buy books or CDs, fill prescriptions or rent cars, someone else, somewhere, is collecting information about them and their transactions. On its own, each bit of information says little about the person being tracked. But combined with health and insurance records, bank loans, divorce records, election contributions and political activities, corporations can create a detailed dossier.

Stanley said most people are unaware how information about them is passed on to government agencies and processed. Although the Privacy Act attempted to put stops on government surveillance, Stanley said that its authors did not anticipate the explosion in private-sector data collection. "It didn't anticipate the growth of data aggregators and the tremendous amount of information that they're able to put together on virtually everyone or the fact that the government could become customers of these companies," Stanley said.

Although the report focused primarily on the flow of data from corporations to the government, data flow actually goes both ways. The government has shared its watch lists with the private sector, opening the way for potential discrimination against customers who appear on the lists. Under section 314 of the Patriot Act, the government can submit a suspect list to financial institutions to see whether the institution has conducted transactions with any individuals or organizations on the list. But once the government shares the list, nothing prevents the institution from discriminating against individuals or organizations on the list.

After the terror attacks of Sept. 11, 2001, the FBI circulated a watch list to corporations that contained hundreds of names of people the FBI was interested in talking to, although the people were not under investigation or wanted by the FBI. Companies were more than happy to check the list against the names of their customers. And if they used the list for other purposes, it's difficult to know. The report notes that there is no way to determine how many job applicants might have been denied work because their names appeared on the list.

"It turns companies into sheriff's deputies, responsible not just for feeding information to the government, but for actually enforcing the government's wishes, for example by effectively blacklisting anyone who has been labeled as a suspect under the government's less-than-rigorous procedures for identifying risks," the report states.

In March 2003 the Technology and Privacy Advisory Committee, created by Secretary of Defense Donald Rumsfeld to examine government data mining, issued a report stating that "rapid action is necessary" to establish clear guidelines for responsible government data mining.

Stanley believes companies are in the initial stages of the Homeland Security gold rush to get government contracts, and that the public and Congress need to do something before policies and practices of private-sector surveillance solidify.

"Government security agencies always have a hunger for more and more information," said Stanley. "It's only natural. It makes it easier for law enforcement if they have access to as much info as they want. But it's crucial that policy makers and political leaders balance the needs of law enforcement and the value of privacy that Americans have always expected and enjoyed."

China Second Most Wired Nation

More than 87 million Chinese were "netizens" in July as China celebrated 10 years of being linked by the Internet to the outside world. The Internet community in China has multiplied 140 times in more than six years, soaring to its current level from just 620,000 users in 1997, the China Internet Information Center (CNNIC) reports. China's Web users surpassed Japan's at the end of 2002, becoming the second largest in the world after the United States, China Daily reports.

Although large in size, the current number represents just 6.6 per cent of the country's total population, leaving room for vast growth. The CNNIC indicated there are 36.3 million computers connected to the Internet, up 17.5 per cent from early 2004. There are almost 626,000 websites, up 32.2 per cent compared with the same period last year. But the report said the digital gulf remains as about 90 per cent of the websites are in the most developed provinces.

Beijing, Southern Guangdong Province, East China's Zhejiang Province and Shanghai are the top four in the number of websites, accounting for 56.8 per cent of the total. The CNNIC also indicated that many government services continue to be provided manually, rather than introducing e-Government. The survey found that only 5.2 per cent of China's government websites are frequently used. Nearly half of the 11,764 government sites are simply one-way mirrors and more interactivity is badly needed.

Most Chinese are using the Web to obtain information, including news, e-books and daily life information. Using the Internet for travel and leisure ranks second among users, over finding new friends, research or sending and receiving e-mails. There is still a large market in China for Internet information and broadband services. The average user sends more than 10 messages via the Internet weekly and the majority (57 per cent) spends less than $1 each month.

Younger people make up the largest group of online customers. People aged 18–24 accounted for 32 per cent of users. People in the 25–30 age bracket make up 29 per cent, and those aged 31–35 account for almost 16 per cent, while those above 35 make up about 16 per cent.

Most broadband users are male technicians, staff in companies or administrative departments, or employees in service industries and commerce. About 30 per cent have high school or college educations. It is expected that many dial-up Internet users may switch in the future, so the prospects for broadband Internet services are promising.

OECD Task Force To Coordinate Fight Against Spam

OECD countries have set up a task force to marshal the efforts of government, business and civil society in the most comprehensive, strategic and inclusive response to date to the problems posed by unsolicited e-mail messages, or spam.

An OECD announcement on August 12 points out that Spam undermines user trust online, reduces productivity, spreads computer viruses and increases costs for all parties, and close international co-operation is essential in order to combat it. At present, a number of countries have several agencies with competencies in tackling spam.

The OECD Task Force will ensure a better focus of work on priority areas and improved coordination between different policy communities. Key objectives will include coordinating international policy responses in the fight against spam, encouraging best practices in industry and business, promoting enhanced tech-

nical measures to combat spam along with improved awareness and understanding among consumers, and facilitating cross-border law enforcement. The initiative promises benefits for developed and developing economies alike.

The creation of the OECD Task Force reflects a consensus that the OECD's broad and inclusive approach, multi-disciplinary expertise and network of contacts with countries and economies outside its membership makes it ideally suited to coordinate and supplement efforts to combat spam at national and international levels.

The Task Force has been given two years to study existing and emerging anti-spam strategies across all sectors; develop and promote an anti-spam tool-kit focused on practical anti-spam strategies, arrangements and solutions; and devise a public awareness strategy in order to support global efforts to combat spam.

As part of their drive against spam, OECD countries will hold an international Workshop on Spam in Busan, Korea on 8–9 September 2004. Following on from a first OECD Workshop on Spam hosted by the European Commission in Brussels on 2–3 February 2004, this will provide a key opportunity for public dialogue on the priorities of the OECD Task Force on Spam.

Hosted by Korea's Ministry of Information and Communication, the Busan workshop will bring together participants from government, industry, civil society and academia. It will be open to the media and to the public, subject to advance registration. Among other things, participants will discuss:

- Next steps in developing an an OECD Anti-spam Toolkit.
- Network management solutions to reduce spam.
- Use of authentication and technical tools to reduce spam.
- How to reduce mobile spam and instant messaging spam.
- Improved co-operation with Asia-Pacific Economic Cooperation (APEC) economies and non-OECD countries in general.

Public contributions to the OECD anti-spam Toolkit may be sent to spam.project@oecd.org.

Least Developed Countries Explore ICT to Escape from Poverty

The first Global ICT Forum for the Least Developed Countries (LDCs), held in Mauritius in August 2004, considered ways to help least developed countries join the Information Society. Organized jointly by the International Telecommunication Union (ITU) and the Commonwealth Business Council and held in association with NEPADs E-Africa Commission, the Forum enabled development partners to hold a series of bilateral and multilateral negotiations on innovative development solutions and practical strategies for deploying ICT projects that can help the worlds poorest countries break away from the poverty trap. More than 150 participants from government, business, civil society and donor agencies took part.

The meeting followed a two-track format: one track set the stage with presentations by the various stakeholders of their expectations, requirements and initiatives, while the other brought together government and small and medium-sized enterprises from the LDCs in one-to-one meetings with development partners to discuss specific areas of cooperation. The Forum gave donors and businesses an opportunity to underscore the current problems of investment in LDCs, while participating governments showed great interest in finding out how to attract financing into their ICT sector. The debate gave rise to a number of policy options that could help increase investment flows into LDC economies.

The novel format of the meeting proved to be extremely effective with the last day organized as a "speed-dating" event where donors, investors and LDCs were given the opportunity to identify, through one-to-one meetings, whether there existed areas of common interest in specific development projects. For example, Mali sought assistance on an e-government project to link 27 ministries through the Internet. USAID, whose assistance programs focus on facilitating the provision of e-government services to increase transparency, particularly in government procurement projects, responded positively to Mali's call.

Lesotho's plea for assistance in strengthening the regulatory skills of the regulatory agency's board members raised positive interest from the African Development Bank, which also showed great interest in financing two SME from Malawi and Mauritius.

The meeting aimed at stimulating positive change. In particular, it examined proposals and models that can be translated into concrete projects mainly in the areas of infrastructure, universal access, education services and entrepreneurship development. It also sought to identify possible sources of funding. In addition to creating a trading platform, the meeting offered an exclusive networking opportunity to participants who were able to gather information and explore possibilities for cooperation in order to build synergies in their LDC-related activities as a way of hedging against risk.

Speaking at the event, Mauritius Acting Prime Minister Jayakrishna Cuttaree said that the borderless nature of ICTs was making the world a global marketplace. "The digital economy has a growth potential for the gross national product of many countries of which LDCs cannot be an exception." He added, "adapting to this new phenomenon within the shortest span of time is the sine qua non condition for getting out of underdevelopment and ensure prosperity."

"Technological developments, if left unmanaged, can widen the current digital gap and trap developing and least developed countries in a perpetual spiral of poverty and exclusion," said Hamadoun I. Tour é, Director of ITUs Telecommunication Development Bureau (BDT). "This is why this multi-stakeholder event is a very important one, not only for LDCs but for all of us trying to make a difference on the ground," he also said. He urged participants to ensure effective cooperation and coordination at all levels in order to achieve the required synergies, complementarities, and efficiencies. Warning governments against over-regulation that can stifle innovation, he urged them to ensure they put in place dynamic but flexible and transparent regulatory regimes. He challenged business leaders to explore the abundant market opportunities that remain untapped in least developed countries. While cautious, he expressed confidence that private sector was now able to develop services in LDCs that have set up adequate regulatory environments with the perspective of an adequate return on their investment.

1. Celebrating Success

The Forum provided an opportunity to showcase a number of success stories with projects jointly implemented by ITU with Sector Members in developing and least developed countries. Among them, the ITU Internet Training Center Initiative implemented in over 50 countries in partnership with Cisco Systems, the ITU Global Telecommunication University supported by Cable & Wireless and the ITU Youth Education Scheme that operates under a partnership arrangement with Vodafone, Anacom of Portugal and NTI of Egypt.

Comoros and Kiribati saw merit of the ITU Internet Training Center initiative for their countries and embarked on discussions with ITU and Cisco to join. A number of participating businesses expressed interest in the ITU Global E-Learning Initiative aimed at providing Internet connectivity to rural schools and e-health services to remote communities in cooperation with Inmarsat and I-Linx. Bhutan's ICTization project aimed at connecting 20 schools and surrounding communities to ICT, has also generated a lot of interest from the Global VSAT Forum, Cisco Systems and Inmarsat. As part of the follow-up activities, ITU will facilitate full-fledge commitments and delivery on the basis of the initial contacts established at the Forum.

Cybercrime Challenge Accelerates After Treaty Ratification

Following the entry into force of the Council of Europe's (COE) Convention on Cybercrime, representatives of some 50 governments met at COE headquarters in Strasbourg, France, in September to consider steps for its full implementation. The convention (treaty) has been signed by 37 governments, including non-member states Canada, Japan, South Africa and the United States, and ratified by 5 members. These are Albania, Croatia, Estonia, Hungary and Lithuania. An additional protocol to the convention, requiring signatories to criminalize the dissemination of racist and xenophobic material through computer systems, was adopted in 2002 by the Committee of Minister of the COE.

The convention is the first international treaty on crimes committed via the Internet and other computer networks, was the result of work by experts from the 45-member COE and several non-member countries. The main aim of the convention – which focuses in particular on child pornography, computer related fraud and violations of network security – is to develop a common criminal policy on cybercrime by promoting international cooperation and adoption of appropriate legislation.

The objectives of the Challenge of Cybercrime conference were to press for rapid ratification by more countries in the "global fight against crime and encourage public-private partnerships in this area; draw attention at the highest political level to the fact that the fight against cybercrme and cyberterrorism should be strengthened, as societies are largely computer-dependent so increasingly vulnerable to cyber attacks; as well as ensure effective implementation of the Cybercrime Convention."

In a background statement, the COE stressed that "computer networks are turning the world into a global information society in which any kind of information is available to Internet users almost anywhere and in which e-Commerce may soon exceed hundreds of billions of Euros. Yet this process is accompanied by an increasing dependency on such networks and a growing vulnerability to criminal intrusion and misuse. Networks facilitate illegal access to information, attacks on private or public computer systems, distribution of illegal content as well as cyber-laundering and possibly cyber-terrorism."

In order to counter these threats, the Conference considered national and international cooperation legal measures to provide for:

- effective criminalization of cyber-offences. Legislation of different countries should be as harmonized as possible to facilitate cooperation.
- investigative and prosecutorial procedures and institutional capacities which allow criminal justice agencies to cope with high-tech crime.
- conditions facilitating direct cooperation between State institutions and between these institutions and the private sector.
- efficient mutual legal assistance regimes, allowing direct cooperation among multiple countries and the establishment of inter-governmental emergency networks.

The text of the Convention, conference report and details on related work of the COE may be found: www.coe.int