I-WAYS, Digest of Electronic Commerce Policy and Regulation 26 (2003) 45–49
IOS Press

In Brief

US Federal and State E-Government 2002 – Greater Security, More Restricted Access

In the wake of the September 11, 2001 terrorist attacks, US Government websites are devoting much greater attention to having security statements online as well as descriptions of their privacy policies, is the main finding of the report, State and Federal E-Government in the United States, 2002 published by Darrel West, Center for Public Policy, Brown University, Providence, Rhode Island. This report presents the third annual update on the features that are available online at American state and federal government websites. See <www.insidepolitics.org/Egovt02us.html>. The differences across the 50 states and between the state and federal governments in 2002 are compared with 2000 and 2001 findings are discussed. Using a detailed analysis of 1,265 state and federal government websites, the author examines the features available online, what variations exist across the country as well as between state and national government sites, and how e-government sites respond to citizen requests for information.

Governments in the US are taking security and privacy much more seriously than they did in 2000 and 2001. This attention to security also has led to an increase in the presence of "restricted areas" on government websites that require registration and passwords for entrance (plus occasionally premium payments). Authorities are creating restricted areas for a variety of reasons, such as an interest in providing premium services, a greater focus on security, personalized service delivery, and bidding on public contracts. West indicates these developments are encouraging the creation of a "two-class" society in regard to e-government. Rather than providing free and open access to all parts of electronic governance, government websites now contain restricted areas and sections requiring premium fees or subscriptions to gain access. These developments raise two types of problems for the future of e-government.

At the same time that government websites are taking privacy very seriously, they also are introducing more clear-cut loopholes in those policies that have the potential to invade the privacy of ordinary individuals. For example, more than a third (35%) of the privacy statements on state and federal websites indicate they share personal information about visitors with legal authorities and law enforcement officers. Most public sector sites (61%) indicate they do not prohibit the commercial marketing of information gained through website visits.

In addition, a "two-class" society of e-government users is emerging that West considers problematic. Six percent of government websites have restricted areas, meaning sections that require a password for entry. One percent have portions that require payment for access to that part of the website. This creates barriers to the free and open access that long has characterized e-government. In the conclusion of the report, the author offers suggestions on how to improve the public navigability and accessibility of government websites.

Online Information

In terms of the availability of basic information at American government websites, it was found that contact information and access to publications and databases were more prevalent in 2002 as compared with previous years. Nearly all sites provide their department's telephone number (96%) which is up from 94% in 2001. The same is true for addresses of the agency in question. Ninety-five percent of agencies listed their addresses, up 2% from 2001. Ninety-three percent of sites provide access to publications while 57% have databases. Seventy-one percent have links to websites outside of government, compared with 69% in 2001.

ISSN 1084-4678/03/$8.00

Services Provided

Fully executable, online service delivery benefits both government and its constituents. In the long run, such services offer the potential for lower cost of service delivery and it makes services more widely accessible to the public, who no longer who have to visit, write or call an agency in order to execute a specific service. As more and more services are put online, e-government will revolutionize the relationship between government and citizens.

Of the web sites examined in 2002, 23% offered services that were fully executable online. This is similar to 25% in 2001. Of the sites examined, 77% provided no services; 12% offered one service, 4% had two services, and 7% had three or more services. There is a great deal of variation in the services available on government websites. The most frequent service is the ability to file taxes online, which was offered by different sites. Other common services included being able to apply for jobs, renew driver's licenses and ordering hunting and fishing licenses.

Privacy and Security

In 2002, 43% of sites have some form of privacy policy, up 28% from 2001. Thirty-four percent now have a visible security policy, up from 18%. These developments have been likely caused by post-September 11 security consciousness. The content of publicly posted privacy and security statements were examined. For privacy policies, several features were identified. These include whether the privacy statement prohibited commercial marketing of visitor information, creation of cookies or individual profiles of visitors, sharing of personal data without prior consent of the visitor, or sharing visitor information with law enforcement authorities. Less than one-third prohibit these activities. In terms of security, 37% of sites say they use computer software to monitor network traffic. This is up 8% from 2001, indicating renewed attention on the part of government officials to the need to protect government websites against hackers and other security threats.

Among other important findings of the research into e-government in the United States are:

- A growing number of sites are offering privacy and security policy statements. This year, 43 % have some form of privacy policy on their site, up from 28% in 2000. Thirty-four percent now have a visible security policy, up from 18% last year.
- Twenty-eight percent of government websites have some form of disability access, up slightly from 27% last year.
- Seven percent of sites offered any sort of foreign language translation feature, up slightly from the 6% found last year.
- Six percent of government websites had restricted areas and one percent have premium features requiring payment for access.
- States vary enormously in their overall ranking based on web presence. Tennessee, New Jersey, California, Connecticut, Pennsylvania, Texas, Washington, Nevada, South Dakota, and Utah ranked highly while Wyoming, Alabama, Mississippi, and Colorado did more poorly.
- In terms of federal agencies, top-rated websites included those by the Federal Communications Commission, Department of Labor, Environmental Protection Agency, Department of Treasury, Department of State, Social Security Administration, and FirstGov (the national government portal), while US circuit courts and the Supreme Court had the lowest ranking sites.
- In general, federal government websites did a better job of offering information and services to citizens than did state government websites.
- Government officials were not as responsive in 2002 as was the earlier in terms of responding to e-mail queries. Whereas 80% answered the sample query in 2001, only 55% did in 2002.

Cybercrime Action Plan Adopted for Asia-Pacific

The Asia-Pacific region is experiencing significant incidents of malicious attacks on the confidentiality, integrity and availability of computer data and systems, a UN organized conference in November 2002 concluded. Computer-related offences such as forgery and fraud, and content-related such as child pornography, and intellectual property rights (IPR) violations, are growing. This also is the case for threats to critical infrastructure and use of the Internet for criminal activity. On a wider scope, the harm inflicted on business, government and industries in Asia-Pacific countries where the Internet is used widely, may impede new applications of ICT.

The UN Economic and Social Commission for Asia and the Pacific (UNESCAP), Ministry of Information and Communication (MIC) of the Republic of Korea, and Korea Information Security Agency (KISA) sponsored the Conference on Cybercrime and Information Security. For details, see <www.apectel.org>. It prepared an Action Plan to raise awareness and combat increasing cybercrime incidents. The overall objective of the Plan is to support, expand and further develop regional responses to cybercrime and information security, in particular through support to the least developed countries, Pacific Island countries and economies in transition of the region. In the short term, it is intended to form the basis for articulating a regional position on cybercrime and information security at the World Summit on Information Society (WSIS) taking place in Geneva in December 2003.

The Plan is designed to contribute to preparing a common understanding among all stakeholders on priority policy actions needed to address existing threats both at the national and regional levels. The vision is an increased number of countries adopting legal and regulatory frameworks to promote information security and cybercrime reduction. Regional arrangements will be encouraged to establish and promote Internet transactions and increased levels of network security.

A program of Guiding Principles was agreed upon: (1) a multi-pronged approach to address the challenges of information security and cybercrime on all fronts – protection, detection and response. Priority will be given to actions in support of preventive approaches; (2) maximum cooperation between the public and private sectors, as well as other stakeholders and members of civil society, is required to successfully meet the challenges; (3) cooperation between more developed and "e-ready" countries is seen as a key mechanism for capacity development and for helping countries to address the challenges of the information society; and (4) respect for the sovereignty of countries as the basis for effective cooperation, constitutional rights of all persons; and (5) human resources development is a basic requirement for detection and response to cybercrime.

Action Plan Framework

Overall Objectives: increased stakeholder awareness and transfer of knowledge; improved policy, legal and regulatory frameworks for promoting information security; establishing regional mechanisms; increased protection against cybercrime; and improved detection and responses to cybercrime.

Stakeholder Awareness: conduct national user campaigns, including young people, educational institutions, consumer and government officials; target the media, engage large private sector corporations and industry associations to sponsor awareness programs; conduct seminars for high-level authorities; and advise less-developed countries on effective systems for detection, protection against, and responses to cybercrime.

Improved Legal and Regulatory Frameworks: Adopt policy and laws consistent with existing international legal instruments that provide for dissuasive sanctions; technical assistance to government to review and assess existing policies, and encourage proactive self-help approaches by the private sector; and enhance willingness to assist in law enforcement investigations.

Regional Mechanisms: Form standing groups and committees of experts to provide advice and give appropriate inputs, as well as help desks for requests for assistance from developing countries, and establish a website to support this activity.

Increased Protection: Make IT security standards and international best practices relating to information security available to governments and the private sector; facilitate sharing of information; and facilitate international assistance to combat cybercrime programs.

Improved Detection: Establish Computer Emergency Response Teams (CERTS), national hotlines for reporting cybercrime; promote codes of conduct; propose mutual assistance regimes; and increase capacity to conduct domestic and transnational electronic investigations.

Strong WTO Ministerial Conference Results Urged

One of the central pillars for liberalizing world trade is by improving market access, the International Chamber of Commerce (ICC) believes. This is considered to be a major driving force for global economic growth, job creation and wider consumer choice. To accomplish these goals, there should be a strong rules-based multilateral trading system built up through the World Trade Organization (WTO). The ICC, on March 31, 2003, prepared a policy statement on trade liberalization objectives that will be transmitted to trade ministers participating in the 5th WTO Ministerial Conference in September 2003 in Cancun, Mexico. In addition to reassuring business that governments are

committed to further liberalize global trade and investment, the ICC is submitting specific policy recommendations for the Ministerial. These range from Intellectual Property Rights, Investment, Trade Facilitation, Government Procurement and Anti-Dumping.

Several recommendations urge WTO action in E-Commerce, Information Technology and Telecommunications. "Current WTO obligations, rules, disciplines and commitments – namely the GATT, GATS and TRIPS agreements – apply to E-Commerce". The ICC has developed the following key principles regarding the negotiations affecting E-Commerce, IT and telecommunications:

- The Reference Paper for basic telecom services should be adopted in full.
- ICC urges all WTO countries to make meaningful market access commitments in both basic telecom and value-added services, and to prevent anti-competitive practices by adhering to the WTO GATS telecom annex for value-added services including Internet services, and which should include full liberalization by a date certain and progressive removal of foreign ownership restrictions.
- WTO members should commit to fully liberalize trade in computer and related services in a way that covers advancing technology and evolving services at a high level of generality.
- Whether considered a good or a service, digital products should continue to flourish in a liberal and open trade environment, with full market access and national treatment, no imposition of discriminatory measures, quantitative restrictions or other trade barriers.
- Where legitimate public policy objectives require domestic regulations that affect E-Commerce, any such regulations should be consistent with existing WTO principles. They should be transparent and non-discriminatory, should represent the least trade-restrictive measures available and should promote an open market environment.
- Intellectual property made available over digital networks should receive strong protection.
- WTO members should commit to fully liberalize trade in services sectors essential to E-Commerce, such as express delivery services, telecom and value-added services, and computer and related services.
- ICC is seeking to make the moratorium on customs duties on electronic transmissions permanent and binding.

APEC Considers Privacy Protection and Transborder Data Flows

The importance of effective consumer privacy protection and uninterrupted transborder data flows for the encouragement of E-Commerce among and between Asia-Pacific Economic Cooperation (APEC) countries was stressed at a Data Privacy Workshop in Chiang Rai, Thailand in February, organized by the E-Commerce Steering Group (ECSG). A "privacy mapping exercise", conducted in 2002 to record policy, legal and self-regulatory approaches to privacy protection in APEC economies, served as the basis for commentaries presented by participants at this Workshop.

Inputs by speakers and participants have been passed on to the ECSG for consideration, in its 2003–2004 program <www.apecsec.org>. Among the main issues will be:

- The need for increased consumer and business sector awareness of the benefits and risks associated with E-Commerce, and of advances in/availability of Privacy Enhancing Technologies. Also, appropriate steps should be taken to ensure data privacy and security protection, including education initiatives on consumer rights and avenues for redress;
- In addressing online privacy protection, a balanced approach must be taken with respect to the protection of data privacy, consumer requests for access to personalized information, goods and services on a 24-7 basis, and their concerns about data privacy. There should be an approach that acknowledges the benefits of the free flow of information in increasingly information-driven economies and the consequences of the misuse of personal information;
- The reality that APEC economies are in different places along the spectrum of developing E-Commerce infrastructures and are addressing related consumer protection issues and enforcement within their jurisdictions, including data privacy issues, and that there are differences in approaches;
- That despite variations across the APEC economies in legal frameworks and policy approaches to data privacy, there are discernible common elements in the approach APEC economies take to defining and implementing data privacy;

- The benefits to cooperation concerning transborder data flows and regarding consumer protection and enforcement matters;
- That APEC economies could benefit from further sharing of information on data privacy approaches and lessons learned, including exploring the commonalities in their approaches and possibilities for accommodation of each others' local laws;
- That there may be benefits to APEC economies in looking at compatible global approaches to privacy protection to ensure cross-border data flow and privacy protection;
- That the OECD privacy guidelines may be a beginning point – not an end point, for discussion of flexible privacy principles, recognizing both their widespread influence and flexibility, but also that review is appropriate in developing guidance due to changes in the information environment since the OECD guidelines were prepared; and
- The unique characteristics and priorities of APEC economies should be taken into account.

The ECSG is expected to consider these points as part of its 2003 work plan. In particular, the results of the privacy mapping exercise will be further examined to identify common elements as well as mechanisms for implementation and enforcement approaches.

OECD Study Calls for Governments to Maintain Telecom Competition Rules

Confidence is slowly returning to the telecommunications sector after the "boom and bust" years of the 1990s, a new OECD concludes. Although the necessary restructuring now underway in the industry is painful, the study shows, governments and regulators are urged to resist the temptation to provide relief to companies by easing competition requirements or by providing financial help.

The study, *After the Telecommunications Bubble*, says that the current state of the industry in OECD countries does not justify a major shift in telecommunications regulatory policy as a way of encouraging new investment. Indeed, competition is still hampered in some market segments, particularly high-speed Internet access, which deprives consumers and businesses of some of the benefits of technological innovation.

The OECD paper adds that the slow return of confidence is being aided by the efforts of companies to strengthen their balance sheets and to renegotiate their debts. The impact of such restructuring on the overall economy of a country is small as the weight of the sector is, in general, relatively limited at between 2 and 4 per cent of gross domestic product. While the effect on equipment suppliers and technology firms has been severe, adjustment in the sector is largely behind us.

Because of robust demand from consumers and businesses, the telecommunications services and equipment sectors should return to steady growth once financial restructuring is completed, the study adds.

It also indicates that the price at which European Union governments auctioned third generation UMTS mobile telephony licenses (about Euro 100 billion altogether) was only one of several factors contributing to the current financial pressure on firms. Recognizing that the prices obtained at the later auctions were far lower than those achieved at the first license sales in Germany and Britain, the study recommends that care should be taken in designing auctions so that they achieve their primary goal of opening markets to competition.

Allowing the spectrum of frequencies allocated for UMTS to be resold by operators as a way of opening up the market to new entrants is recommended. But the study urges caution. Changing the rules over secondary market trading after allocating rights could be seen as providing the equivalent of a government subsidy as those rights could become more valuable than the prices set at the auctions.

After the Telecommunications Bubble, which draws on work to be published in the forthcoming OECD Communications Outlook in May 2003, will appear as a special chapter in the OECD's forthcoming Economic Outlook No. 73.