Order Code 98-67 STM

Report for Congress

Distributed by Penny Hill Press http://pennyhill.com

Internet: An Overview of Key Technology Policy Issues Affecting Its Use and Growth

Updated August 9, 2002

Marcia S. Smith, John D. Moteff, Lennard G. Kruger,
Glenn J. McLoughlin, and Jeffrey W. Seifert
Resources, Science, and Industry Division

Internet: An Overview of Key Technology Policy Issues Affecting Its Use and Growth

Summary

The growth of the Internet may be affected by a number of issues being debated by the 107th Congress. This report summarizes several key technology policy issues.

1. **Internet privacy** issues encompass concerns about information collected by Web site operators, and, separately, about the extent to which law enforcement officials or employers monitor an individual's Internet activities. The new anti-terrorism law, the USA PATRIOT Act (P.L. 107-56) has privacy advocates concerned about new authorities granted to law enforcement officials in that regard.

2. Concerns about **computer security** are prevalent in both the government and private sectors. Concerns have also been raised about the vulnerability of the nation's critical infrastructures (e.g. electrical power supply) to cyber attacks. Issues for the 107th Congress include oversight and improvement of the protection of federal computer systems and cooperation with and between the private sectors.

3. **Broadband Internet access** gives users the ability to send and receive data at speeds far greater than current Internet access over traditional telephone lines. With deployment of broadband technologies beginning to accelerate, Congress is seeking to ensure fair competition and timely broadband deployment to all sectors and geographical locations of American society.

4. Since the mid-1990s, commercial transactions on the Internet—called **electronic commerce (e-commerce)**—have grown substantially. Among the issues facing Congress are encryption procedures to protect e-commerce transactions, extension of the 3-year tax moratorium on domestic e-commerce taxation, the impact of the USA PATRIOT Act, and how the policies of the European Union (EU) and World Trade Organization (WTO) may affect U.S. e-commerce activities.

5. Unsolicited commercial electronic mail (UCE), or "**junk e-mail**" or "spam," aggravates many computer users because it is a nuisance and the cost may be passed on to consumers through higher charges from Internet service providers who must upgrade their systems to handle the traffic. Proponents of UCE insist it is a legitimate marketing technique and protected by the First Amendment.

6. The administration and governance of the **Internet's domain name system** (DNS) is currently under transition from federal to private sector control. The 107th Congress is monitoring how the Department of Commerce is managing and overseeing this transition in order to ensure competition and promote fairness among all Internet constituencies.

7. The growing role of the Internet in the political economy of the United States is attracting attention in the 107th Congress. Three major themes characterize legislative activity and interest: Internet infrastructure development, resource management, and the provision of online services by the government (called "**e-government**").

Contents

Introduction 1

Internet Privacy 1
- Collection of Data by Web Site Operators and Fair Information Practices . . 2
  - Commercial Web Sites 2
  - Federal Web Sites 4
- Monitoring of E-Mail and Web Activity 5
  - Law Enforcement Monitoring 5
  - Employer Monitoring 6
- Spyware 7
- Consumer Identity Theft and Protecting Social Security Numbers 7

Computer Security 8

Broadband Internet Access 13
- Easing Restrictions and Requirements on Incumbent Telephone Companies 13
- Federal Assistance for Broadband Deployment 15

Electronic Commerce 15
- Background 15
- The E-Commerce Industry 16
- E-Commerce Policies: 1998-2001 17
- Issues for the Bush Administration and the 107th Congress 17
  - Protection and Security Issues 18
  - E-Commerce Taxation 18
  - The EU and WTO 19

Unsolicited Commercial Electronic Mail ("Junk E-Mail" or "Spam") 20

Internet Domain Names 21

Government Information Technology Management 26
- Internet Infrastructure and National Policy 26
  - Information Technology R&D 27
- Information Resource Management: The Role of a Federal CIO 27
- Provision of Online Services (E-Government) 30

Appendix A: Legislation Pending in the 107th Congress 32
- Internet Privacy 32
- Computer Security 33
- Broadband Internet Access 33
- Electronic Commerce 34
- Junk E-Mail 35
- Internet Domain Names 35
- Government Information Technology Management 35

Appendix B: List of Acronyms 36

Appendix C: Legislation Passed by the 105th and 106th Congresses 39

Appendix D: Related CRS Reports 44

Internet: An Overview of Key Technology Policy Issues Affecting Its Use and Growth

Introduction

The continued growth of the Internet for personal, government, and business purposes may be affected by a number of issues being debated by Congress. Among them are Internet privacy, computer security, access to broadband (high-speed) services, electronic commerce (e-commerce), unsolicited commercial electronic mail ("junk e-mail" or "spam"), Internet domain names, and government information technology management. Lists of pending legislation, acronyms, related legislation passed in the 105th and 106th Congresses, and other CRS reports that provide more detail on the issues are included as appendices.

Internet Privacy[1]

Internet privacy issues encompass a range of concerns. One is that the Internet makes it easier for governmental and private sector entities to obtain information about consumers and possibly use that information to the consumers' detriment. That issue focuses on the extent to which Web site operators collect personally identifiable information (PII) about individuals and share that information with third parties, often without the knowledge or consent of the people concerned.

Another aspect of Internet privacy is the extent to which Internet activities such as electronic mail (e-mail) and visits to Web sites are monitored by law enforcement officials or employers. In the wake of the September 11 terrorist attacks, the issue of law enforcement monitoring of Internet activity has become more controversial, with some advocating additional tools for law enforcement to fight terrorism, and others cautioning that basic tenets of our democracy, such as privacy, not be sacrificed in the effort.

Congress passed a law in 1998 protecting the privacy of children under 13 as they use commercial Web sites (the Children's Online Privacy Protection Act, P.L. 105-277). The only subsequent legislation that has passed regarding protection of PII concerns the use of "cookies" by federal government, not commercial, Web sites. Those laws are the FY2001 Transportation Appropriations Act (P.L. 106-346), the

---

[1] CRS Report RL31408, *Internet Privacy: Overview and Pending Legislation*, by Marcia S. Smith, provides an overview of Internet privacy issues and tracks pending legislation. It is updated more frequently than this report. CRS Report RL30784, *Internet Privacy: An Analysis of Technology and Policy Issues*, by Marcia S. Smith, provides more comprehensive analysis of many of the issues involved in this debate.

FY2001 Treasury-General Government Appropriations (P.L. 106-554), and the FY2002 Treasury-General Government Appropriations Act (P.L. 107-67). As for law enforcement monitoring of Internet and e-mail activities, Congress passed the USA PATRIOT Act (P.L. 107-56) in the wake of the September 11, 2001 terrorist attacks. That law expands the authorities for law enforcement officials to monitor such activities.

The 107th Congress continues to have a strong interest in Internet privacy issues. CRS Report RL31408, *Internet Privacy: Overview and Pending Legislation*, tracks pending legislation. Medical records privacy and financial records privacy are not Internet privacy issues. For information on those topics, see CRS Report RS21221, *A Brief Summary of the Medical Privacy Rule*, and CRS Report RS20185, *Privacy Protection for Customer Financial Information*, respectively. Consumer identity theft also is not an Internet privacy issue per se, but often arises in that context because of the perception that Social Security numbers and credit card numbers are more readily accessible because of the Internet. Therefore it is mentioned below.

Collection of Data by Web Site Operators and Fair Information Practices

Perhaps the most often discussed Internet privacy issue is whether commercial Web sites should be required to adhere to four "fair information practices" proposed by the Federal Trade Commission (FTC): providing *notice* to users of their information practices before collecting personal information, allowing users *choice* as to whether and how personal information is used, allowing users *access* to data collected and the ability to contest its accuracy, and ensuring *security* of the information from unauthorized use. In particular, the question is whether industry can be relied upon to regulate itself, or if legislation is needed to protect consumer privacy. Questions also have arisen about whether federal government Web sites should have to adhere to such practices. CRS Report RL30784, *Internet Privacy: An Analysis of Technology and Policy Issues*, provides more detailed information on fair information practices in the Internet context.

Commercial Web Sites. The FTC has been very active on Internet privacy issues for several years. Based on a series of surveys of commercial Web sites each year since 1997, the FTC has issued reports and made recommendations about whether legislation is needed to protect consumer privacy on the Web. Although the FTC and the Clinton Administration favored self regulation, in 1998, frustrated at industry's slow pace, the FTC announced that it would seek legislation protecting children's privacy on the Internet by requiring parental permission before a Web site could request information about a child under 13. The Children's Online Privacy Protection Act (COPPA, part of P.L. 105-277) was enacted four months later.

In 1999, the FTC concluded that further legislation was not needed at that time for children or adults, but reversed its decision in 2000 when another survey indicated that industry still was not self regulating to the desired extent. The FTC voted 3-2 to propose legislation that would allow it to establish regulations requiring Web site operators to follow the four fair information practices. The close vote

underscored the controversial nature of the FTC's reversal of position, which was further illuminated at a Senate Commerce Committee hearing on May 25, 2000.

In June 2001, Timothy Muris replaced Robert Pitofsky as FTC chairman. On October 4, 2001, Mr. Muris gave a speech revealing his position on the issue. He does not see a need for additional legislation now, preferring strong enforcement of existing regulations coupled with industry self-regulation instead.

The Internet industry has taken steps to demonstrate that it can self regulate. One example is the formation of the Online Privacy Alliance (OPA), a group of more than 80 companies and associations in the Internet business. OPA developed a set of privacy guidelines and its members are required to adopt a privacy policy, post it on their site(s), and implement the policy. Another is the establishment of "seals" for Web sites by the Better Business Bureau, TRUSTe, and WebTrust. To display a seal from one of those organizations, a Web site operator must agree to abide by certain privacy principles (some of which are based on the OPA guidelines), a complaint resolution process, and to being monitored for compliance. Another approach is using software called "P3P" (Platform for Privacy Preferences) that gives individuals the option to allow their web browser to match the privacy policies of websites they access with the user's selected privacy preferences. Advocates of self regulation argue that these efforts demonstrate industry's ability to police itself. Advocates of further legislation argue that while the seal programs are useful, they do not carry the weight of law, limiting remedies for consumers whose privacy has been violated. They also point out that while a site may disclose its privacy policy, that does not necessarily equate to having a policy that protects privacy.

Four bills (H.R. 89, H.R. 237, H.R. 347, and S. 2201) are pending specifically on the topic of protecting the PII of Web site visitors. H.R. 4678 is a broader consumer privacy protection bill. The Senate-passed version of the bankruptcy reform bill (S. 420) prohibits (with exceptions) companies, including Web site operators, that file for bankruptcy from selling or leasing PII obtained in accordance with a policy that said such information would not be transferred to third parties, if that policy was in effect at the time of the bankruptcy filing. A modified version of this language is included in the conference version of the bill (H.R. 333, H. Rept. 107-617). H.R. 2135 would limit the disclosure of personal information (defined as PII and sensitive personal information) by information recipients in general, and S. 1055 would limit the commercial sale and marketing of PII. Congressional attention is currently focused on H.R. 4678 and S. 2201. CRS Report RL31408 provides a comparison of those two bills in its appendix.

In a related measure, S. 2839 (Cleland) seeks to protect the privacy of children using elementary or secondary school or library computers that use "Internet content management services,"such as filtering software to restrict access to certain Web sites. Under that bill, Internet content management service providers must notify local school or library authorities of their policies regarding collection, use, and disclosure of information from or about children, and notify those authorities if the policies change. The bill also prohibits such services from collecting personal information from or about a child, and amends the Children's Online Privacy Protection Act to include Internet content management service providers in the definition of "operator."

Federal Web Sites. Until the summer of 2000, attention was focused on privacy issues associated with commercial Web sites. That changed in June 2000, however, when controversy erupted over the privacy of visitors to government Web sites. The issue concerned federal agencies' use of computer "cookies"(small text files placed on users' computers when they access a particular Web site) to track activity at their Web sites. Federal agencies had been directed by President Clinton and the Office of Management and Budget (OMB) to ensure that their information collection practices adhere to the Privacy Act of 1974. A September 5, 2000 letter from OMB to the Department of Commerce further clarified that "persistent" cookies, which remain on a user's computer for varying lengths of time (from hours to years), are not allowed unless four specific conditions are met. "Session" cookies, which expire when the user exits the browser, are permitted.

In June 2000, however, the Clinton White House announced that it had just learned that contractors for the Office of National Drug Control Policy (ONDCP) had been using cookies to collect information about those using ONDCP's Web site during an anti-drug campaign wherein users clicking on anti-drug ads on various Web sites were taken to an ONDCP site. Cookies then were placed on users' computers to count the number of users, what ads they clicked on, and what pages they viewed on the ONDCP site. The White House directed ONDCP to cease using cookies, and OMB issued a memorandum reminding agencies to post and comply with privacy policies and detailing the limited circumstances under which agencies should collect personal information.

Congress reacted to the overall concern about federal agency information practices on Web sites by adding language concerning such activities by departments and agencies funded in the FY2001 Treasury-General Government Appropriations Ac, commonly called the "Treasury-Postal Appropriations Act." The language was contained both in the FY2001 Treasury-Postal Appropriations Act itself, and in the FY2001 Transportation Appropriations Act. Section 501 of the FY2001 Transportation Appropriations Act (P.L. 106-346) prohibited funds in the FY2001 Treasury-Postal act from being used by any federal agency to collect, review, or create aggregate lists that include personally identifiable information (PII) about an individual's access to or use of a federal Web site or enter into agreements with third parties to do so, with exceptions. Similar language is included in the FY2002 Treasury-Postal Appropriations Act (P.L. 107-67), and in the FY2003 Treasury-Postal Appropriations bill (H.R. 5120/S. 2740).

Section 646 of the FY2001 Treasury-Postal act, as included in the FY2001 Consolidated Appropriations Act (P.L. 106-554), required Inspectors General (IGs) of agencies or departments to report to Congress within 60 days of enactment on activities by those agencies or departments relating to collection of PII about individuals who access any Internet site of that department or agency, or entering into agreements with third parties to obtain PII about use of government or non-government Web sites. Senator Thompson released two reports in April and June 2001 based on the findings of agency IGs who discovered unauthorized persistent cookies and other violations of government privacy guidelines on several agency Web sites. An April 2001 GAO report (GAO-01-424) on implementation of federal guidance for agency use of cookies concluded that most of the 65 sites it reviewed were following OMB's guidance. S. 851 (Thompson) would establish an 18-month

commission to study the collection, use, and distribution of personal information by federal, state, and local governments. H.R. 583 (Hutchinson) would create a commission to study privacy issues more broadly. S. 2629 (Torricelli) would provide a framework for ensuring effective data and privacy management by federal agencies. Section 218 of S. 803 (Lieberman), which passed the Senate June 27, 2002, would set requirements on government agencies in how they assure the privacy of PII in government information systems, and establish privacy guidelines for federal Web sites. S. 2201, reported from the Senate Commerce Committee August 1, 2002 (S. Rept. 107-240), *inter alia* requires federal agencies that are Internet Service Providers or Online Service Providers, or operate Web sites, to provide notice, choice, access, and security in a manner similar to what the bill requires for non-governmental entities, with exceptions.

Monitoring of E-Mail and Web Activity

Law Enforcement Monitoring. Another Internet privacy storm broke in the summer of 2000 when it became known that the FBI, with a court order, installs software on Internet Service Providers' equipment to intercept e-mail and monitor an individual's Web activity. The extent to which that software program, originally called Carnivore, can differentiate between e-mail and Web activity involving a subject of an FBI investigation and other people's e-mail and Web activity is of considerable debate, with critics claiming that Carnivore violates the privacy of innocent users. A House Judiciary subcommittee held a hearing on Carnivore on July 24, 2000. Legislation that would have, *inter alia,* required law enforcement to report on its use of e-mail intercepts was discussed at a September 6, 2000 Senate Judiciary hearing. No legislation cleared the 106th Congress, however. The FBI later renamed the program "DCS 1000." The FY2002 Department of Justice authorization bill (H.R. 2215) as passed by the House and Senate requires the Justice Department to report to Congress on its use of DCS 1000 or any similar system.

Following the September 11 terrorist attacks, attention focused on whether law enforcement officials required new tools to combat terrorism, including additional authority to monitor Internet activity. After several weeks of debate, Congress passed and the President signed into law the USA PATRIOT Act (P.L. 107-56) that does just that. Civil liberties groups have expressed concern about the potential ramifications of the new Act on this and other grounds. They assert that they will monitor law enforcement use of the new powers to determine if any need to be challenged in court. In summary, Title II of P.L. 107-56 —

- expands the scope of subpoenas for records of electronic communications to include records commonly associated with Internet usage, such as session times and duration (Section 210);
- *allows* ISPs to divulge records or other information (but not the contents of communications) pertaining to a subscriber if they believe there is immediate danger of death or serious physical injury or as otherwise authorized, and *requires* them to divulge such records or information (excluding contents of communications) to a governmental entity under certain conditions. It also allows an ISP to divulge the *contents* of communications to a law enforcement agency if it reasonably believes that an emergency involving immediate

danger of death or serious physical injury requires disclosure of the information without delay (Section 212);

- adds routing and addressing information (used in Internet communications) to dialing information to the information a government agency may capture using pen registers and trap and trace devices as authorized by court order, while excluding the content of any wire or electronic communications (Section 216). The section also requires law enforcement officials to keep certain records when they use their own pen registers or trap and trace devices and to provide those records to the court that issued the order within 30 days of expiration of the order. To the extent that Carnivore-like systems fall with the new definition of pen registers or trap and trace devices provided in the Act, that language would increase judicial oversight of the use of such systems; and
- allows a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from a protected computer under certain circumstances.

Section 224 sets a 4-year sunset period for many of the Title II provisions, but among the sections excluded from the sunset are Sections 210 and 216.

Privacy advocates worried that, in an emotionally charged climate, Congress would pass legislation that it later will regret. Groups such as the American Civil Liberties Union (ACLU), Center for Democracy and Technology (CDT), and Electronic Privacy Information Center (EPIC) urge caution, fearful that, in an attempt to track down and punish the terrorists who threaten American democracy, one of the fundamental tenets of that democracy—privacy—may itself be threatened. CDT's Executive Director said [http://www.cdt.org/press/011025press.shtml]: "This bill has been called a compromise but the only thing compromised is our civil liberties." The implications for Internet privacy of the new law are discussed in CRS Report RL31289, *The Internet and the USA PATRIOT Act: Potential Implications for Electronic Privacy, Security, Commerce, and Government.*

H.R. 3482 would amend the USA PATRIOT Act and, *inter alia*, lower the threshold for when ISPs may divulge the contents of communications, and to whom, as permitted under Section 212 of that Act. See CRS Report RL31408 for more information.

S. 2846 would create a Commission on Enhancing Security and Preserving Freedom to investigate standards for using, selecting, and operating investigative and surveillance technologies to meet law enforcement and national security needs so as to best preserve the personal dignity, liberty, and privacy of individuals, and the advisability of creating a government entity or procedures to ensure such technologies are used in that manner.

Employer Monitoring. An emerging issue is whether employers should be required to notify their employees if e-mail or other computer-based activities are monitored. A 2001 American Management Association survey, which is available at [http://www.amanet.org/press/amanews/ems2001.htm], found that 62.8% of the companies surveyed monitor Internet connections, 46.5% store and review e-mail, and 36.1% store and review computer files. The public policy concern appears to be

less about whether companies should be able to monitor activity, but whether they should notify their employees of that monitoring.

Spyware

Some software products include, as part of the software itself, a method by which information is collected about the use of the computer on which the software is installed. When the computer is connected to the Internet, the software periodically relays the information it has collected back to the software manufacturer or a marketing company. The software that performs the collection and reporting function is often called "spyware." Software programs that include spyware can be obtained on a disk or downloaded from the Internet. They may be sold or provided for free. Typically, users have no knowledge that the software product they are using includes spyware. Some argue that users should be notified if the software they are using includes spyware. Two bills (H.R. 112 and S. 197) have been introduced in the 107th Congress to require such notification.

Another use of the term spyware refers to software that can record a person's keystrokes on a computer keyboard. In this way, all typed information can be obtained by another party, even if the author modifies or deletes what was written, or if the characters do not appear on the monitor (such as when entering a password). Commercial products have been available for some time, but the existence of such software was highlighted in 2001 when the FBI used it in a case against Mr. Nicodemo Scarfo, Jr. on charges of illegal gambling and loan sharking. Law enforcement officials armed with a search warrant reportedly installed spyware (called "key logging" software in this context) on Mr. Scarfo's computer, allowing them to obtain his password for an encryption program he used, and thus to obtain evidence. Some privacy advocates argue wiretapping authority should have been obtained, rather than a search warrant, for use of such software since it intercepts communications. Law enforcement officials are reluctant to provide details of the software to prove their contention that no communications were intercepted and hence a search warrant was sufficient. More recently, press reports have indicated that the FBI is developing a program dubbed "Magic Lantern," which performs a similar task, but can be installed on a subject's computer remotely by surreptitiously including it in an e-mail message, for example. Privacy advocates are questioning what type of legal authorization would be required for use of such techniques.

Consumer Identity Theft and Protecting Social Security Numbers

The widespread use of computers for storing and transmitting information is thought by some to be contributing to consumer identity theft, in which one individual assumes the identity of another using personal information such as credit card and Social Security numbers. Government agencies report sharply increasing numbers of consumer identity theft cases, but whether the Internet is responsible is debatable. Some attribute the rise instead to carelessness by businesses in handling personally identifiable information, and by credit issuers that grant credit without proper checks. The FTC found that less than 1% of identity theft cases are linked to

the Internet (*Computerworld,* February 12, 2001, p. 7). The FTC has a toll-free number (877-ID-THEFT) to help victims of identity theft.

Although not related directly to whether Social Security numbers are more accessible because of the Internet, it should be noted that the 105th Congress passed the Identity Theft and Assumption Deterrence Act (P.L. 105-318). That Act sets penalties for persons who knowingly, and with the intent to commit unlawful activities, possess, transfer, or use one or more means of identification not legally issued for use to that person. Also, the 106th Congress passed the Social Security Number Confidentiality Act (P.L. 106-433, H.R. 3218) which prohibits the display of SSNs on unopened checks or other Treasury-issued drafts. Furthermore, the 106th Congress passed the Internet False Identification Act (P.L. 106-578), which updates existing law against selling or distributing false IDs to include those sold or distributed through computer files, templates, and disks.

Several bills have been introduced in the 107th Congress relating to identity theft or protection of Social Security numbers (H.R. 91, H.R. 220, H.R. 1478, H.R. 2036/S.1014, S. 848, H.R. 3053/S. 1399, and S. 1742). H.R. 4678 also has provisions regarding identity theft. Hearings have been held on some of these bills. S. 848 was reported from the Senate Judiciary Committee on May 16, 2002 and referred to the Senate Finance Committee. S. 1742 was reported from Senate Judiciary on May 21, 2002.

Computer Security

As use of the Internet grows, so has concern about security of and on the Internet. Widespread media attention to a long list of security-related incidents (e.g. the Melissa virus, the Love Bug, denial-of-service attacks, and the Code Red, Code Red II, and Nimda worms) represents the tip of the iceberg. Every day, persons gain access, or try to gain access, to someone else's computer without authorization to read, copy, modify, or destroy the information contained within. These persons range from juveniles to disgruntled (ex)employees, to criminals, to competitors, to politically or socially motivated groups, to agents of foreign governments.

The extent of the problem is unknown. Much of what gets reported as computer "attacks" are probes, often conducted automatically with software widely available for even juveniles to use. But the number of instances where someone has actually gained unauthorized access is not known. Not every person or company whose computer system has been compromised reports it either to the media or to authorities. Sometimes the victim judges the incident not to be worth the trouble. Sometimes the victim may judge that the adverse publicity would be worse. Sometimes the affected parties don't even know their systems have been compromised.

There is some evidence to suggest, however, that the number of incidents is increasing. According to the Computer Emergency Response Team (CERT) at Carnegie-Mellon University, the number of incidents reported to it has grown just about every year since the team's establishment—from 132 incidents in 1989 to almost 23,000 incidents in 2000. In just the first half of 2001, over 15,000 incidents have been reported. The Computer Security Institute (CSI), in cooperation with the

Federal Bureau of Investigation (FBI), has conducted an annual survey since 1996. For those responding to the question of whether they have experienced unauthorized use of their computer systems in the last 12 months, the percentage answering yes has risen from 42% in 1996 to 85% in 2001.[2]

The impact on society from the unauthorized access or use of computers is also unknown. Again, some victims may choose not to report losses. In many cases, it is difficult or impossible to quantify the losses. But social losses are not zero. Trust in one's system may be reduced. Proprietary and/or customer information (including credit card numbers) may be compromised. Any unwanted code must be found and removed. The veracity of the system's data must be checked and restored if necessary. Money may be stolen from accounts or extorted from the victim. If disruptions occur, sales may be lost. If adverse publicity occurs, future sales may be lost and stock prices may be affected. Estimates of the overall financial losses due to unauthorized access vary and their accuracy is untested. Estimates typically range in the billions of dollars per major event like the Love Bug virus or the denial-of-service attacks in February 2000. Similar estimates have been made for the Code Red worms. Estimates of losses internationally range up to the tens of billions of dollars. Those able and willing to estimate financial losses in the 2000 CSI/FBI survey estimated a total of $378 million in losses in the previous 12 months.[3]

Aside from the losses discussed above, there is also growing concern that unauthorized access to computer systems could pose an overall national security risk should it result in the disruption of the nation's critical infrastructures (e.g., transportation systems, banking and finance, electric power generation and distribution). These infrastructures rely increasingly on computer networks to operate, and are themselves linked by computer and communication networks. To address this concern, President Clinton issued a Presidential Decision Directive (PDD-63) in May 1998. PDD-63 set as a national goal the ability to protect critical infrastructures from intentional attacks (both physical and cyber) by 2003. It set up organizational and operational structures within the federal government to help achieve this goal and called for a coordinated effort to engage the private sector. (See CRS Report RL30153, *Critical Infrastructures: Background and Early Implementation of PDD-63*). The Bush Administration has chosen to follow a similar policy as articulated in Executive Order 13231, but has set up a slightly different organizational structure for coordinating that policy and its implementation. In its June 2002 proposal to establish a Department of Homeland Security, a number of the organizations established by PDD-63 would be transferred to the new Department and the Department would become yet another player in developing and implementing computer security policy and programs.

---

[2] The CSI/FBI survey is not a scientific sampling of the nation's computer systems. Surveys are sent to computer security practitioners in U.S. corporations and government agencies. In 2001, 538 surveys were sent out; 532 respondents answered the question about unauthorized use.

[3] 64% of the 2001 CSI/FBI survey respondents acknowledged financial losses; 35% of them could quantify those losses. These percentages are down from the previous year, but the total estimated losses are about $100 million greater. A majority of the losses were attributed to loss of proprietary information and fraud.

As a deterrent, the federal computer fraud and abuse statute, 18 U.S.C. 1030, makes it a federal crime to gain unauthorized access to federal government computers, to be exposed to certain information contained on government computers, to damage or threaten to damage federal computers, bank computers, or computers used in interstate commerce, to traffic in passwords for these computers, to commit fraud from these computers, or from accessing a computer to commit espionage. The statute also provides for penalties. For more information on this statute, see CRS Report 97-1025, *Computer Fraud and Abuse: An Overview of 18 U.S.C. 1030 and Related Federal Criminal Laws*. Most states also have laws against computer fraud and abuse. The USA PATRIOT Act (P.L. 107- 56), passed in the wake of the September 11 terrorist attacks, increased some of the penalties associated with these illegal activities. The Act also permits a single warrant to be granted to allow investigators to track hackers across jurisdictions.

At the international level, the 41-country Council of Europe is negotiating a treaty to facilitate tracking cyber criminals across national boundaries. The final draft of the treaty was completed in June 2001. The United States was an observer at these negotiations. U.S. businesses have expressed some concern about their liability and the costs associated with record-keeping under this treaty. A discussion of the treaty can be found on the Council's web page, at [http://conventions.coe.int/treaty/EN/cadreprojets.htm].[4]

While the tools for prosecuting appear to be in place, most experts agree that much more can be done to make the Internet and its users more secure. The federal government is required to protect sensitive information on its own computers. The Computer Security Act of 1987 authorizes the National Institute of Standards and Technology (NIST) to develop standards to be used by agencies to protect non-national security oriented computers (the National Security Agency does the same for classified information and national security systems) and requires agencies to develop and implement security programs and plans to protect the information on their computers. The Paperwork Reduction Act of 1995 gives OMB the responsibility to oversee the development and implementation of computer security standards, programs, and plans. OMB offers agencies guidance on how to meet their requirements with OMB Circular A-130, Appendix III.

The General Accounting Office (GAO) has found that federal agencies are not consistently good at protecting certain computer systems (typically those used in financial management).[5] GAO has concluded that part of the problem is that there is not strong government wide oversight. As part of the FY2001 Defense Authorization Act (P.L. 106-398), Congress passed the Federal Information Security

---

[4] There is also some debate within the international community about what to do about computer intrusions by government agents; for example, whether such acts would be considered acts of war. For more information regarding this issue, see CRS Report RL30735, *Cyberwarfare*.

[5] U.S. General Accounting Office, *Computer Security. Weaknesses Continue to Place Critical Federal Operations and Assets at Risk*. Testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives. GAO-01-600T. April 5, 2001.

Reform Act. The Act puts into statute much of OMB Circular A-130 guidance. It also strengthens oversight by requiring agencies to have independent reviews of their security programs and plans annually and to report the results of those reviews to OMB. In turn, OMB is to report to Congress on the results.

The security of private-sector computer systems varies. Some industries have been at the forefront of security (e.g. banking and finance), while others are just now appreciating the threat to and vulnerabilities of their systems. In response to PDD-63, some of the sectors that operate critical infrastructures have formed Information Sharing and Analysis Centers (ISACs) and across sectors they have formed the Partnership for Critical Infrastructure Security. The goal of these associations is to learn from each other's experiences and to quickly respond to new attacks and vulnerabilities. It should be noted, too, that in addition to CERT at Carnegie Mellon, individual security firms and security-related associations offer clearinghouses for security-related news, alerts, warnings, etc. The informal networks by which security information spreads is also very extensive.

The market for computer and Internet security (divided into hardware, software, and service providers) is large and growing. The CSI/FBI survey cites a 1999 International Data Corporation (IDC) estimate that the security software industry will grow from $2 billion to $7.4 billion by 2003 and the security hardware market will grow from $500 million to $1.9 billion by 2003. According to Redherring.com (*Picking the Locks on the Internet Security Market*, [http://www.Redherring.com], July 24, 2000), the security services market is expected to grow from $7 billion to $14 billion by 2003. Operating systems and applications developers say they are paying greater attention to designing better security into their products. But still, it is common to have vulnerabilities found in products after they have been put on the market. In some cases, patches have had to be offered at the same time a new product is brought onto the market. And, although patches are offered to fix these vulnerabilities in most cases, many system administrators do not keep their software/configurations current. Many intrusions take advantage of vulnerabilities noted many months earlier, for which fixes have already been offered.

There are as yet no industry standards for determining how secure a firm's computer system should be or for assessing how secure it is in fact. However, there is a push by the major accounting houses and insurance firms to make corporate leaders and boards more accountable for their firms' information assets. Also, some observers speculate that it is only a matter of time before owners of computer systems are held responsible for damages done to third-party computers as a result of inadequately protecting their own systems.[6] Nor are there any standards on how secure a vendor's software should be. The federal government, in cooperation with a number of other countries, has developed a set of International Common Criteria for Information Technology Security Evaluation, to allow certified laboratories to test security products and rate their level of security for government use. These criteria may evolve into industry standards for certifying security products.

---

[6] See Computerworld. *IT Security Destined for the Courtroom*. May 21, 2001. Vol 35. No. 21. p 1,73.

A number of issues are confronting the 107th Congress during its second session. Congress continues to oversee agencies' performance in meeting their obligations under the Computer Security Act, OMB Circular A-130 and now the Federal Information Security Reform Act. Also, Congress may inquire about the Bush Administration's restructuring of information security coordination. Some Members have also expressed an interest in how much research and development the federal government is doing to better secure computer systems. Congress may take up legislation that would grant an explicit Freedom of Information Act (FOIA) exemption for computer system security information shared between the private sector and the federal government. Finally, Congress may face questions about how to strike a balance between its efforts to promote Internet privacy and Internet security. While one cannot protect privacy without security, there are some who fear that without proper checks, efforts to promote security could come at the expense of privacy. On the other hand, as the health care industry and the financial industry prepare to meet new privacy regulations and guidelines, the costs associated with ensuring privacy (via greater access controls, etc.) may become an issue.

A number of bills were introduced that touch upon one aspect of Internet security or another. H.R. 1259 (Morella) would expand somewhat the responsibilities of the National Institute of Standards and Technology (NIST) in developing computer security standards, to promote the use of commercial security products and to track the use of commercial products by federal agencies. The bill would also require NIST to maintain a list of security products that are certified to conform to standards developed by NIST. It also authorizes NIST to perform evaluations of agency information security programs and to report the findings of those evaluations to Congress. H.R. 1292 (Skelton), the Homeland Security Strategy Act of 2001, calls for the President to develop a Homeland Security Strategy that protects the territory, critical infrastructure, and citizens of the United States from the threat or use of chemical, biological, radiological, nuclear, cyber or conventional weapons. H.R. 1158 (Thornberry, modified and reintroduced as H.R. 4660 in the second session) would establish a Department of National Homeland Security. This has been eclipsed by H.R. 5005 (Army). A comparable bill was introduced in the Senate (S. 1534, Lieberman, modified and reintroduced as S. 2452). H.R. 2435 (Davis) provides Freedom of Information Act (FOIA) and anti-trust protections for information relating to computer and network security that is shared with and between the private sector and the federal government. S. 1456 (Bennett) would provide similar protections. H.R. 3394 (Boehlert), the Cyber Security Research and Development Act, would authorize $880 million over the next five years to NSF and NIST to support research, establish programs, and provide fellowships in computer security to individual researchers, universities, and community colleges. S. 1900 (Edwards) would authorize NIST to award a grant to a non-governmental entity to develop cybersecurity best practices and to support long-term research in cybersecurity. S. 1901 (Edwards) would establish an NSF fellowship program and a sabbatical program in cybersecurity to help attract new faculty into this area of research. S. 2182 (Wyden) would establish research grant programs in cybersecurity at NSF and NIST. The bill would also establish grants to allow institutions of higher learning build and improve upon their cybersecurity programs. H.R. 3844 (Davis) would replace the sunsetting Government Information Security Reform Act (GISRA). This bill more or less follows GISRA with some modifications. It also authorizes NIST to define different levels of information security that agencies must

use to protect various categories of information. These categories, too, are to be defined by NIST. A number of these bills have been eclipsed by or added as amendments to the bills to establish a Department of Homeland Security (H.R. 5005, S. 2542). FOIA exemptions language has been added to both bills. Elements of H.R. 3844 have been added to H.R. 5005. A simple GISRA reauthorization, which eliminates the sunset provision, has been added to a Senate E-Government bill (S. 803).

Broadband Internet Access[7]

Broadband Internet access gives users the ability to send and receive data at speeds far greater than conventional "dial up" Internet access over existing telephone lines. New broadband technologies—cable modem, digital subscriber line (DSL), satellite, and fixed wireless Internet—are currently being deployed nationwide by the private sector. Concerns in Congress have arisen that while the number of new broadband subscribers continues to grow, the rate of broadband deployment in urban and high income areas appears to be outpacing deployment in rural and low-income areas, thereby creating a potential "digital divide" in broadband access. The Telecommunications Act of 1996 authorizes the Federal Communications Commission (FCC) to intervene in the telecommunications market if it determines that broadband is not being deployed to all Americans in a "reasonable and timely fashion."

At issue is what, if anything, should be done at the federal level to ensure that broadband deployment is timely, that industry competes on a level playing field, and that service is provided to all sectors of American society. The debate in the 107th Congress has centered on two approaches: easing certain legal restrictions and requirements (imposed by the Telecommunications Act of 1996) on incumbent telephone companies that provide high-speed data (broadband) access; and providing federal financial assistance for broadband deployment in rural and economically disadvantaged areas.

Easing Restrictions and Requirements on Incumbent Telephone Companies. The debate over access to broadband services has prompted policymakers to examine a range of issues to ensure that broadband will be available on a timely and equal basis to all U.S. citizens. One issue under examination is whether present laws and subsequent regulatory policies as they are applied to the ILECs (incumbent local exchange [telephone] companies such as SBC or Verizon (formerly known as Bell Atlantic)) are thwarting the deployment of such services. Two such regulations are the restrictions placed on Bell operating company (BOC) provision of long distance services within their service territories, and network unbundling and resale requirements imposed on all incumbent telephone companies. In the 107th Congress, H.R. 1542 (Tauzin-Dingell) would lift these restrictions and requirements, with some exceptions, for high speed data (broadband) transmission. H.R. 1542 was passed by the House on February 27, 2002. After passage of H.R.

---

[7] See also CRS Issue Brief IB10045, *Broadband Internet Access: Background and Issues*, by Lennard G. Kruger and Angele A. Gilroy, which is updated more frequently than this report.

1542, deregulatory legislation was introduced by Senators Breaux and Nickles in the Senate. S. 2430, introduced on April 30, 2002, seeks to encourage broadband deployment by requiring the FCC to establish "regulatory parity" among the various providers of broadband. Similarly, S. 2863, introduced by Senator McCain on August 2, 2002, would lift regulations on residential broadband service. For more information on broadband legislation, see CRS Issue Brief IB10045, *Broadband Internet Access: Background and Issues.*

Those supporting the lifting or modification of restrictions claim that action is needed to promote the deployment of broadband services, particularly in rural and under served areas. Present regulations contained in Sections 271 and 251 of the 1996 Telecommunications Act, they claim, are overly burdensome and discourage needed investment in broadband services. According to proponents, unbundling and resale requirements, when applied to advanced services, provide a disincentive for ILECs to upgrade their networks, while BOC interLATA data restrictions unnecessarily restrict the development of the broadband network. ILECs, they state, are the only entities likely to provide these services in low volume rural and other under served areas. Therefore, proponents claim, until these regulations are removed the development and the pace of deployment of broadband technology and services, particularly in unserved areas, will be lacking. Furthermore, supporters state, domination of the Internet backbone market is emerging as a concern and entrance by ILECs (particularly the BOCs) into this market will ensure that competition will thrive with no single or small group of providers dominating. Proponents also cite the need for regulatory parity; cable companies who serve approximately 70 percent of the broadband market are not subject to these requirements. Additional concerns that the lifting of restrictions on data would remove BOC incentives to open up the local loop to gain interLATA relief for voice services are also unfounded, they state. The demand by consumers for bundled services and the large and lucrative nature of the long distance voice market will, according to proponents, provide the necessary incentives for BOCs to seek relief for interLATA voice services.

On the other hand, opponents claim that the lifting of restrictions and requirements will undermine the incentives needed to ensure that the BOCs and the other ILECs will open up their networks to competition. Present restrictions, opponents claim, were built into the 1996 Telecommunications Act to help ensure that competition will develop in the provision of telecommunications services. Modification of these regulations, critics claim, will remove the incentives needed to open up the "monopoly" in the provision of local services. Competitive safeguards such as unbundling and resale are necessary, opponents claim, to ensure that competitors will have access to the "monopoly bottleneck" last mile to the customer. Therefore, they state the enactment of legislation to modify these provisions of the 1996 Telecommunications Act will all but stop the growth of competition in the provision of local telephone service. A major change in existing regulations, opponents claim, would not only remove the incentives needed to open up the local loop but would likely result in the financial ruin of providers attempting to offer competition to incumbent local exchange carriers. As a result, consumers will be hurt, critics claim, since the hoped-for benefits of competition such as increased consumer choice and lower rates will never emerge. Concern over the inability of regulators to distinguish between provision of voice only and data services if BOC interLATA restrictions for data services and ILEC unbundling and resale

requirements for advanced services are lifted was also expressed. Opponents also dismiss arguments that BOC entrance into the marketplace is needed to ensure competition. The marketplace, opponents claim, is a dynamic one but proposed deregulation would unsettle nascent competition in the market.

Federal Assistance for Broadband Deployment. Other legislation introduced in the 107th Congress would provide grants, loans, and tax credits for broadband deployment, particularly in rural and/or low income areas. A comprehensive loan and grant package (S. 2448) was introduced by Senator Hollings on May 2, 2002. S. 2448 would use monies from the telephone excise tax to provide loans and grants to spur broadband deployment in rural and underserved areas, to stimulate demand for broadband services, and to fund next generation broadband technology research and development. Meanwhile, the Farm Security and Rural Investment Act of 2002 (P.L. 107-171, signed by the President on May 13, 2002) authorizes the Secretary of Agriculture to make loans and loan guarantees to eligible entities for facilities and equipment providing broadband service in rural communities. Section 6103 authorizes a total of $100 million through FY2007 ($20 million for each of fiscal years 2002 through 2005, and $10 million for each of fiscal years 2006 and 2007).

Broadband tax credits are another approach. S. 88 (the Broadband Internet Access Act, introduced by Senator Rockefeller) would provide a 10% credit for deploying "current generation" broadband equipment in rural and underserved areas, and a 20% credit for "next generation" broadband equipment deployment for rural and underserved areas and for all residential broadband subscribers. Legislative language similar to S. 88 was attached to the Senate version of the 2001 economic stimulus bill, and contemplated (but ultimately not attached) as an amendment to the Senate energy bill. It is possible that broadband tax credit language could be attached to other major legislation in the Senate before adjournment. For more information on federal assistance for broadband deployment, please see CRS Report RL30719, *Broadband and the Digital Divide: Federal Assistance Programs*.

Electronic Commerce[8]

Background

The convergence of computer and telecommunications technologies has revolutionized how we get, store, retrieve, and share information. Many experts contend that this convergence has created the Information Economy, driven by the Internet, and fueled a surge in U.S. productivity and economic growth. Commercial transactions on the Internet, whether retail business-to-customer or business-to-business, are commonly called electronic commerce, or "e-commerce."

---

[8] See also CRS Report RS20426, *Electronic Commerce: An Introduction*, by Glenn J. McLoughlin, which is updated more frequently than this report.

Since the mid-1990s, commercial transactions on the Internet have grown substantially.[9] By 1996, Internet traffic, including e-commerce, was doubling every 100 days. By mid-1997, the U.S. Department of Commerce reported that just over 4 million people were using e-commerce; by the end of 1997, that figure had grown to over 10 million users. Business conducted over the Internet continues to grow, even with an economic slowdown and with many new "dot-com" businesses no longer in existence. A January 2001 study by the Pew Internet and American Life Project found that overall, 29 million American shoppers made purchases on-line during the fourth quarter of 2001, spending an average of $392, up from $330 in the fourth quarter of 2000. A quarter of all Internet users did some shopping on the Internet this year, up from one-fifth of Internet users last year. Of those e-commerce shoppers, 58 percent were women; this is the first time that more women than men have been reported using the Internet for retail e-commerce.

Internationally, there are issues regarding Internet use and e-commerce growth. While the western industrialized nations dominate Internet development and use, by the year 2003 more than half of the material posted on the Internet will be in a language other than English. This has large ramifications for e-commerce and ease of transactions, security, and privacy issues. Policymakers, industry leaders, academicians, and others are concerned that this development will not correlate with equal access to the Internet for many in developing nations—therefore creating a global "digital divide." The United States and Canada represent the largest percentage of Internet users, at 56.6%. Europe follows with 23.4%. At the end of 2000, of approximately 200 million Internet users worldwide, only 3.1% are in Latin America, 0.5% are in the Middle East, and 0.6% are in Africa. The Asian Pacific region has 15.8% of all Internet users; but its rate of growth of Internet use is nearly twice as fast as the United States and Canada. In this respect, the U.S.-Canada share of Internet use may decline to 36% by 2005.

The E-Commerce Industry

Even with some concern about accuracy and timeliness of e-commerce statistics, reliable industry sources report huge jumps in e-commerce transactions, particularly during fourth quarter holiday shopping. But long-term, industry growth has not been limited to just holiday shopping. According to a study undertaken by the University of Texas, the Internet portion of the U.S. economy grew at a compounded rate of 174% from 1995-1998 (the U.S. gross domestic product grew at 2.8% during the same period), and e-commerce accounted for one-third of that growth. Increasingly, many firms use "vortals"—vertically integrated portals or gateways that advertise or provide information on a specific industry or special interest. As a portion of e-commerce business, vortals provide targeted advertising for e-commerce transactions, and may grow from 35% of all e-commerce advertising to 57% by 2004.

---

[9] For statistics and other data on e-commerce, see: CRS Report RL30435, *Internet and E-Commerce Statistics: What They Mean and Where to Find Them On the Web.* Other sources include: [http://www.idc.com], [http://www.abcnews.go.com], [http://www.forrester.com], [http://www.emarketer.com], and [http://www.cs.cmu.edu]. It is important to note that some measurements of e-commerce, particularly that data reported in the media, have not been verified.

However, not all firms providing these services are profitable; in fact, most have yet to turn a profit.

One of the fastest growing sectors of e-commerce is business-to-business transactions–what is often called "B2B." This sector continues to expand, even in the current economic downturn. The Forrester Group, a private sector consulting firm, estimates that by 2003, that sector of the U.S. economy will reach $1.5 trillion, up from nearly $200 billion in 2000. Business-to-business transactions between small and medium sized businesses and their suppliers is rapidly growing, as many of these firms begin to use Internet connections for supply chain management, after-sales support, and payments.

E-Commerce Policies: 1998-2001

The Clinton Administration advocated a wide range of policy prescriptions to encourage e-commerce growth. These included calling on the World Trade Organization (WTO) to declare the Internet to be a tax-free environment for delivering both goods and services; recommending that no new tax policies be imposed on Internet commerce; stating that nations develop a "uniform commercial code" for electronic commerce; requesting that intellectual property protection—patents, trademarks, and copyrights—be consistent and enforceable; that nations adhere to international agreements to protect the security and privacy of Internet commercial transactions; that governments and businesses cooperate to more fully develop and expand the Internet infrastructure; and that businesses self-regulate e-commerce content.

The Clinton Administration's "The Emerging Digital Economy" (April 1998), "The Emerging Digital Economy II" (June 1999), "Digital Economy 2000" (June 2000), and "Leadership for the New Millennium, Delivering on Digital Progress and Prosperity" (January 2001) provided overarching views on domestic and global e-commerce. These reports provide data on the explosive growth of e-commerce, its role in global trade and national Gross Domestic Product (GDP), and contributions that computer and telecommunications technology convergence is making to productivity gains in the United States and worldwide. The Administration also argued that the effects that information technologies have had on raising national productivity, lowering inflation, creating high wage jobs, and contributing up to one-third of all domestic growth in the 1990s.

Issues for the Bush Administration and the 107th Congress

Since the mid-1990s, Congress also has taken an active interest in e-commerce issues. Among the many issues, Congress may revisit policies that establish federal encryption procedures and provide electronic security in the wake of September 11, 2001. The 107th Congress has passed a bill that would extend the moratorium on domestic e-commerce taxation to November 2003. In addition, congressional policymakers are looking at the European Union (EU) and WTO policies and regulations in e-commerce.

Protection and Security Issues. There are a variety of protection and security issues that affect e-commerce growth and development. *Encryption* is the encoding of electronic messages to transfer important information and data, in which "keys" are needed to unlock or decode the message. Encryption is an important element of e-commerce security, with the issue of who holds the keys at the core of the debate. In September 1999, United States announced plans to further relax its encryption export policy by allowing export of unlimited key length encryption products, with some exceptions. It also advocated reduced reporting requirements for those firms that export encrypted products. The rules for implementing this policy were issued in September 2000 by the Bureau of Export Administration in the Department of Commerce. However, the events of September 11, 2001 have caused many in industry and government to review this policy–and the USA PATRIOT ACT of 2001 (P.L. 107-56) has given lawmakers greater authority to gain access to electronic financial transactions (for example, to ferret out illegal money laundering). Consumers and civil liberties activists are very concerned about this development and have said they will monitor this law closely.

In a related area, the 106th Congress considered and passed legislation establishing standards for transmission and verification of electronic transmissions. *Electronic signatures* are a means of verifying the identity of a user of a computer system to control access to, or to authorize, a transaction. The main congressional interests in electronic signatures focus on enabling electronic signatures to carry legal weight in place of written signatures, removing the inconsistencies among state policies that some fear may retard the growth of e-commerce, and establishing federal government requirements for use of electronic signatures when filing information electronically. Neither federal law enforcement nor national security agencies oppose these objectives, and most U.S. businesses would like a national electronic signatures standard to further enhance e-commerce. When President Clinton signed into law the Electronic Signatures in Global and National Commerce Act (P.L. 106-229), the process of developing a national electronic signature standards was begun. Among its many provisions, this law also establishes principles for U.S. negotiators to follow for setting global electronic signatures policies.

E-Commerce Taxation. Congress passed the Internet Tax Freedom Act on October 21, 1998, as Titles XI and XII of the Omnibus Consolidated and Emergency Supplemental Appropriations Act of 1999 (P.L. 105-277, 112 Stat 2681). Among its provisions, the Act imposes a 3-year moratorium on the ability of state and local governments to levy certain taxes on the Internet; it prohibits taxes on Internet access, unless such a tax was generally imposed and actually enforced prior to October 1, 1998; it creates an Advisory Commission on Electronic Commerce (ACEC), which may make recommendations to Congress on e-commerce taxation in the United States and abroad; and it opposes regulatory, tariff, and tax barriers to international e-commerce and asks the President to pursue international agreements to ban them.) The ACEC made its policy recommendations, after much debate and some divisiveness, to Congress on April 3, 2000. The ACEC called for, among its recommendations, extending the domestic Internet tax moratorium for five more years, through 2006; prohibiting the taxation of digitized goods over the Internet, regardless of national source; and a continued moratorium on any international tariffs on electronic transmissions over the Internet.

Congressional interest in Internet taxation has weighed concerns about impeding the growth of e-commerce by taxing revenues; enforcement and compliance of an Internet tax; and policies outside of the United States which do not impose an Internet tax. H.R. 1552, The Internet Tax Nondiscrimination Act (Rep. Cox) would extend the Internet tax moratorium through November 1, 2003. It was passed by both houses of Congress and signed into law on November 28, 2001 (P.L. 107-75; see also: Report RS20980, *Internet Tax Bills in the 107th Congress: A Brief Comparison*, for more information.)

The EU and WTO. While much of the debate on the government's role in e-commerce has focused on domestic issues in the United States, two important players—the EU and the WTO—will likely have an important impact on global e-commerce policy development. The EU is very active in e-commerce issues. In some areas there is agreement with U.S. policies, and in some areas there are still tensions. While the EU as an entity represents a sizable portion of global Internet commerce, across national boundaries, Internet use and e-commerce potential varies widely. Supporters state that e-commerce policy should not be set by EU bureaucrats in Brussels. Therefore, the EU has approached e-commerce with what one observer has called a "light regulatory touch." Among contentious issues, the EU has supported the temporary moratorium on global e-commerce taxes, and supports making the moratorium permanent. But the EU has taken a different approach than U.S. policy by treating electronic transmissions (including those that deliver electronic goods such as software) as services. This position would allow EU countries more flexibility in imposing trade restrictions, and would allow treating electronic transmissions—including e-commerce—as services, making them subject to EU value-added duties. The EU also has taken a different approach to data protection and privacy, key components for strengthening e-commerce security and maintaining consumer confidence. The EU actions prohibit the transfer of data in and out of the EU, unless the outside country provides sufficient privacy safeguards. The U.S. position is to permit industry self-regulation of data protection and privacy safeguards. (For more information on the European data directive, see CRS Report RL30784, *Internet Privacy: An Analysis of Technology and Policy Issues*.)

The WTO has presented another set of challenges to U.S. policymakers. The first two WTO ministerial meetings addressed issues that have an impact on e-commerce. The first WTO Ministerial conference was held in Singapore on December 9-13, 1996. Among the issues considered by the WTO participants was an agreement to reduce trade barriers for information technology goods and services. This issue was considered vital to the development of telecommunications infrastructure–including the Internet–among developing nations. A majority of participants signed an agreement to reduce these barriers. At the second WTO Ministerial conference, held in Geneva on May 18 and 20, 1998, an agreement was reached by the participating trade ministers to direct the WTO General Council to develop a work program on electronic commerce and to report on the progress of the work program, with recommendations, at the next conference. The ministers also agreed that countries continue the practice of not imposing tariffs on electronic transmission. While e-commerce was on the agenda at the third WTO conference in Seattle in 1999, disruptions at that conference curtailed discussions.

The WTO also has addressed e-commerce. In the October 27 draft Ministerial Declaration for the fourth conference in Doha, Qatar, the Chairman of the General Council stated that "electronic commerce creates new challenges and opportunities for trade for Members of all stages of development...[W]e instruct the General Council to consider the most appropriate institutional changes for handling the Work Programme, and to report on further progress to the Fifth Ministerial Conference" and that "Members will maintain their current practice of not imposing custom duties on electronic transmissions until the Fifth Session." This language was adopted as article 34 under the Ministerial Declaration of November 14, 2001. Upcoming WTO conferences may address any additional e-commerce issues raised by WTO working groups on goods, services, intellectual property and economic development; or address related e-commerce issues raised at previous ministerial conferences in areas such as privacy, security, taxation, and infrastructure. (See CRS Report RS20319, *Telecommunications Services Trade and the WTO Agreement* and CRS Report RS20387, *The World Trade Organization (WTO) Seattle Ministerial Conference).*

Unsolicited Commercial Electronic Mail ("Junk E-Mail" or "Spam")[10]

One aspect of increased use of the Internet for electronic mail (e-mail) has been the advent of unsolicited commercial e-mail (UCE), also called junk e-mail, spam, or unsolicited bulk e-mail. The *Report to the Federal Trade Commission of the Ad-Hoc Working Group on Unsolicited Commercial Email* [http://www.cdt.org/spam] reviews the issues in this debate.

In 1991, Congress passed the Telephone Consumer Protection Act (P.L. 102-243) that prohibits, *inter alia*, unsolicited advertising via facsimile machines, or "junk fax" (see CRS Report RL30763, *Telemarketing: Dealing with Unwanted Telemarketing Calls*). Many question whether there should be an analogous law for computers, or at least some method for letting a consumer know before opening an e-mail message whether or not it is unsolicited advertising and to direct the sender to cease transmission of such messages.

Opponents of junk e-mail such as the Coalition Against Unsolicited Commercial Email (CAUCE) argue that not only is junk e-mail annoying, but its cost is borne by consumers, not marketers. Consumers are charged higher fees by ISPs that must invest resources to upgrade equipment to manage the high volume of e-mail, deal with customer complaints, and mount legal challenges to junk e-mailers. CAUCE's founder, Ray Everett-Church, is cited in the January 31, 2001 edition of *Newsday* as saying that some ISPs estimate that spam costs consumers about $2-3 per month. Some want to prevent bulk e-mailers from sending messages to anyone with whom they do not have an established business relationship, treating junk e-mail the same way as junk fax. Proponents of unsolicited commercial e-mail argue that it is a valid method of advertising. The Direct Marketing Association (DMA), for example, argues that instead of banning unsolicited commercial e-mail, individuals should be

---

[10] See also CRS Report RS20037, *"Junk E-Mail": An Overview of Issues and Legislation Concerning Unsolicited Commercial Electronic Mail ("Spam")*, by Marcia S. Smith, which is updated more frequently than this report.

given the opportunity to notify the sender of the message that they want to be removed from its mailing list—or "opt-out." In January 2000, the DMA launched a new service, the E-mail Preference Service, where any of its members that send UCE must do so through a special Web site where consumers who wish to "opt out" of receiving such mail can register themselves [http://www.e-mps.org]. Each DMA member is required to check its list of intended recipients and to delete those consumers who have opted out. While acknowledging that the service will not stop all spam, the DMA considers it "part of the overall solution" (see [http://www.the-dma.org/aboutdma/release4.shtml]). Critics argue that most spam does not come from DMA members, so the DMA plan is insufficient.

To date, the issue of restraining junk e-mail has been fought primarily over the Internet or in the courts. Some ISPs will return junk e-mail to its origin, and groups opposed to junk e-mail will send blasts of e-mail to a mass e-mail company, disrupting the company's computer systems. Filtering software also is available to screen out e-mail based on keywords or return addresses. Knowing this, mass e-mailers may avoid certain keywords or continually change addresses to foil the software, however. In the courts, ISPs with unhappy customers and businesses that believe their reputations have been tarnished by misrepresentations in junk e-mail have brought suit against mass e-mailers.

Although several bills were debated in both the 105th and 106th Congresses, no legislation cleared Congress. Some states are passing their own legislation. According to the "Spamlaws" Website [http://www.spamlaws.com], 25 states have enacted spam laws. The 107th Congress remains interested in the issue at the federal level. Five bills have been introduced to date: H.R. 95 (Green), H.R. 718 (Wilson), H.R. 1017 (Goodlatte), H.R. 3146 (C. Smith), and S. 630 (Burns). H.R. 2472 (Lofgren) is not a spam bill per se, but would require marks or notices on e-mail forwarded to minors that contains sexually oriented advertising. H.R. 718 has been reported from the House Energy and Commerce Committee (H.Rept. 107-41, Part 1) and the House Judiciary Committee (H.Rept. 107-41, Part 2). The two versions are quite different. The Senate Commerce Committee ordered reported S. 630 on May 17, 2002. For more details, see CRS Report RS20037.

Internet Domain Names[11]

The 107th Congress continues to monitor issues related to the Internet domain name system (DNS). Internet domain names were created to provide users with a simple location name for computers on the Internet, rather than using the more complex, unique Internet Protocol (IP) number that designates their specific location. As the Internet has grown, the method for allocating and designating domain names has become increasingly controversial.

The Internet originated with research funding provided by the Department of Defense Advanced Research Projects Agency (DARPA) to establish a military

---

[11] See also CRS Report 97-868, *Internet Domain Names: Background and Policy Issues*, by Lennard G. Kruger, which is updated more frequently than this report.

network. As its use expanded, a civilian segment evolved with support from the National Science Foundation (NSF) and other science agencies. No formal statutory authorities or international agreements govern the management and operation of the Internet and the DNS. Prior to 1993, NSF was responsible for registration of nonmilitary generic Top Level Domains (gTLDs) such as .com, .org, and .net. In 1993, the NSF entered into a 5-year cooperative agreement with Network Solutions, Inc. (NSI) to operate Internet domain name registration services. With the cooperative agreement between NSI and NSF due to expire in 1998, the Clinton Administration, through the Department of Commerce (DOC), began exploring ways to transfer administration of the DNS to the private sector.

In the wake of much discussion among Internet stakeholders, and after extensive public comment on a previous proposal, the DOC, on June 5, 1998, issued a final statement of policy, *Management of Internet Names and Addresses* (also known as the "White Paper"). The White Paper stated that the U.S. government was prepared to recognize and enter into agreement with "a new not-for-profit corporation formed by private sector Internet stakeholders to administer policy for the Internet name and address system." On October 2, 1998, the DOC accepted a proposal for an Internet Corporation for Assigned Names and Numbers (ICANN). On November 25, 1998, DOC and ICANN signed an official Memorandum of Understanding (MOU), whereby DOC and ICANN agreed to jointly design, develop, and test the mechanisms, methods, and procedures necessary to transition management responsibility for DNS functions to a private-sector not-for-profit entity.

The White Paper also signaled DOC's intention to ramp down the government's Cooperative Agreement with NSI, with the objective of introducing competition into the domain name space while maintaining stability and ensuring an orderly transition. During this transition period, government obligations will be terminated as DNS responsibilities are transferred to ICANN. Specifically, NSI committed to a timetable for development of a Shared Registration System that permits multiple registrars to provide registration services within the .com, .net., and .org gTLDs. NSI (now VersiSign) will continue to administer the root server system until receiving further instruction from the government.

Significant disagreements between NSI on the one hand, and ICANN and DOC on the other, arose over how a successful and equitable transition would be made from NSI's previous status as exclusive registrar of .com, org. and net. domain names, to a system that allows multiple and competing registrars. On November 10, 1999, ICANN, NSI, and DOC formally signed an agreement which provided that NSI (now VeriSign) was required to sell its registrar operation by May 10, 2001 in order to retain control of the dot-com registry until 2007. In April 2001, arguing that the registrar business is now highly competitive, VeriSign reached a new agreement with ICANN whereby its registry and registrar businesses would not have to be separated. With DOC approval, ICANN and VeriSign signed the formal agreement on May 25, 2001. The agreement provides that VeriSign will continue to operate the .org registry until 2002; the .net registry until June 30, 2005 (which prior to that time will be opened for recompetition unless market measurements indicate that an earlier expiration date is necessary for competitive reasons); and the .com registry until at least the expiration date of the current agreement in 2007, and possibly beyond. VeriSign agreed to enhanced measures (including annual audits arranged by ICANN

and made available to the U.S. government) to ensure that its registry-operation unit gives equal treatment to all domain name registrars, including VeriSign's registrar business.

Meanwhile, on September 4, 2000, ICANN and the DOC agreed to extend their MOU until September 30, 2001 or sooner, if both parties agree that the work set under the MOU has been completed. The MOU has subsequently been extended to September 30, 2002. Remaining tasks, many of which are underway, include: creating new Internet top-level domains, completing selection of the ICANN Board of Directors, enhancing the architecture of the root-name server system, formalizing contractual relationships between ICANN and the regional Internet Protocol address registries, and establishing stable arrangements between ICANN and the organizations responsible for the operation of country-code Top-Level Domains (TLDs).

The Department of Commerce (DOC) remains responsible for monitoring the extent to which ICANN satisfies the principles of the White Paper as it makes critical DNS decisions. The DOC has asked ICANN to provide information on its transition and reform efforts in order to help DOC decide whether to renew, extend, or modify the MOU agreement that expires September 30, 2002. Congress remains keenly interested in how the Administration manages and oversees the transition to private sector ownership of the DNS. A February 2002 proposal by ICANN's President to radically restructure ICANN (see below) led the Congress to call for oversight hearings. An oversight hearing held by the Senate Commerce, Science and Transportation Committee on June 12, 2002 focused on ICANN reform and the role of the DOC in ensuring that reform. A bipartisan letter from the House Energy and Commerce Committee to the Secretary of Commerce calls for only a short term renewal of the DOC-ICANN Memorandum of Understanding (set to expire September 30, 2002) until ICANN institutes reforms that ensure greater accountability and transparency. A letter from the Senate Republican High Tech Task Force also urges heightened DOC scrutiny of the DOC-ICANN MOU and cites concerns that ICANN has become an unaccountable regulatory body.

Two key issues addressed by ICANN are the addition of new top level domains and the election of At-Large Board members. At its July 16, 2000 meeting in Yokohama, the ICANN Board of Directors adopted a policy for the introduction of new top-level domains (TLDs), which could expand the number of domain names available for registration by the public. After considering a total of 47 applications, the ICANN Board selected seven companies or organizations each to operate a registry for one of seven new TLDs, as follows: .biz, .aero, .name, .pro, .museum, .info, and .coop. ICANN's selection of new TLDs has proven controversial. Critics assert that the TLD selection process was inappropriately subjective, insufficiently transparent, and lacking in adequate due process procedures. In its defense, ICANN argues that the selection process was sufficient to meet its goal of expeditiously selecting a limited number of diverse TLDs, and that these will serve as an initial and experimental "proof of concept" phase in order to ensure that new TLDs can be introduced in the future without undermining the stability of the Internet. In August 2001, the Chairmen and Ranking Members of the Energy and Commerce Committee and the Telecommunications Subcommittee sent a letter to the Secretary of Commerce urging DOC to encourage ICANN to speed its process for selecting

additional TLDs. Meanwhile, ICANN is considering eleven applications for operating .org after the current agreement with VeriSign expires on December 31, 2002. The ICANN Board is expected to select the winning application in September 2002.

Meanwhile, legislation introduced by Rep. Shimkus on June 28, 2001 (H.R. 2417) sought to create a "kids-friendly top level domain name" that would contain only age-appropriate content. Ideally, parents would then be able to restrict their children's access to inappropriate material by installing filters on their computers, allowing only the viewing of approved web pages within the ".kids" domain. On November 1, the House Energy and Commerce Committee held a hearing on proposed substitute language that would direct DOC (via NTIA) to create a second level .kids domain within the .us country code TLD. The .us domain is owned by the DOC, which recently contracted its operation to a private company, NeuStar (which opened the entire .us TLD to the American public on April 24, 2002). NeuStar has also proposed the creation of a .kids.us domain as part of its contract with DOC. The revised legislation, reintroduced as the Dot Kids Implementation and Efficiency Act of 2002 (H.R. 3833) was passed by the House on May 21, 2002 and authorizes NTIA to require the .us registry (currently NeuStar) to establish, operate, and maintain a second level domain within the .us TLD that is restricted to material suitable for minors.

An identical Dot Kids bill, S. 2537, was introduced by Senator Dorgan into the Senate on May 21, 2002. Also in the Senate, S. 2137 (Family Privacy and Security Act) was introduced by Senator Landrieu on April 16 to require NTIA to compel ICANN to establish a new TLD exclusively for material harmful to minors (for example, a .xxx or .adult domain). All websites with material harmful to minors would then be required to migrate to the new domain. Another bill introduced into the House (H.R. 4658, Truth in Domain Names Act, introduced by Rep. Pence on May 2) would make it a punishable crime to false or misleading domain names to attract children to Internet sites not appropriate for children.

Regarding the composition of ICANN's board of directors, ICANN bylaws call for an international and geographically diverse 19-member board of directors, composed of a president, nine at-large members, and nine members nominated by three Supporting Organizations representing Domain Name, Address, Internet Protocol constituencies. At ICANN's March 2000 meeting in Cairo, the sitting board agreed to a plan whereby five At-Large board members, one from each of five geographic regions of the world, would be directly elected by Internet users. On October 10, 2000 ICANN announced the five new At-Large board members elected by over 34,000 Internet users. At the November 2000 annual meeting, ICANN initiated a study to determine how to select the remaining At-Large board members. The At Large Membership Study Committee (ALSC) released its report and recommendations on November 5, 2001. The ALSC recommended that only domain name holders be eligible to vote for at large board members, and that the number of at-large members on the board be reduced from nine to six. At ICANN's March 2002 meeting in Ghana, the board opted not to conduct another round of elections to replace the five At-Large board members elected in October 2000 (and whose terms expire in November 2002). Meanwhile, the President of ICANN, Stewart Lynn, has issued a report calling for significant reform of ICANN's governing structure. On

June 22, 2002, ICANN released a "Blueprint for Reform," which calls for a significant restructuring of ICANN. Specifically, the Board of Directors would be composed of fifteen members: the ICANN President, eight members appointed by a nominating committee, and six selected by three Supporting Organizations. The reform blueprint also recommends that ICANN collect a fee of 25 cents per registered domain name. The reform proposal was approved at the June 28 ICANN Board meeting in Bucharest. A detailed implementation plan will be developed and considered at the October 2002 Board meeting in Shanghai. Some in the Internet community have spoken against the ICANN reform proposal, asserting that its elimination of elected At-Large board members precludes effective representation of unaffiliated Internet users.

Another issue surrounding the DNS is the resolution of trademark disputes that arise in designating domain names. In the early years of the Internet, when the primary users were academic institutions and government agencies, little concern existed over trademarks and domain names. As the Internet grew, however, the fastest growing number of requests for domain names were in the .com domain because of the explosion of businesses offering products and services on the Internet. Since domain names have been available from NSI on a first-come, first-serve basis, some companies discovered that their name had already been registered. The situation was aggravated by some people (dubbed "cybersquatters") registering domain names in the hope that they might be able to sell them to companies that place a high value on them.

The increase in conflicts over property rights to certain trademarked names has resulted in a number of lawsuits. The White Paper called upon the World Intellectual Property Organization (WIPO) to develop a set of recommendations for trademark/domain name dispute resolutions, and to submit those recommendations to ICANN. At ICANN's August 1999 meeting in Santiago, the board of directors adopted a dispute resolution policy to be applied uniformly by all ICANN-accredited registrars. Under this policy, registrars receiving complaints will take no action until receiving instructions from the domain-name holder or an order of a court or arbitrator. An exception is made for "abusive registrations" (i.e. cybersquatting and cyberpiracy), whereby a special administrative procedure (conducted largely online by a neutral panel, lasting 45 days or less, and costing about $1000) will resolve the dispute. Implementation of ICANN's Domain Name Dispute Resolution Policy commenced on December 9, 1999.

WIPO initiated a second study which produced recommendations on how to resolve disputes over bad faith, abusive, misleading or unfair use of other types of domain names such as personal names, geographical terms, names of international organizations, and others. WIPO released its second report on September 3, 2001, recommending that generic drug names be canceled upon complaint and that international intergovernmental organization names be subject to a dispute resolution process. However, WIPO did not recommend new rules regarding personal, geographical, or trade names. WIPO has decided to subject its second report to a comprehensive analysis by its Standing Committee on the Law of Trademarks, Industrial Designs and Geographical Indications. The analysis is expected to be completed by mid-2002.

Meanwhile, the 106th Congress took action, passing the Anticybersquatting Consumer Protection Act (incorporated into P.L. 106-113, the FY2000 Consolidated Appropriations Act). The Act gives courts the authority to order the forfeiture, cancellation, and/or transfer of domain names registered in "bad faith" that are identical or similar to trademarks. The bill would also provide for statutory civil damages of at least $1,000, but not more than $100,000, per domain name identifier. In the 107th Congress, legislation has been introduced (H.R. 4640, introduced by Rep. Coble on May 2) which would provide criminal penalties for providing false information in registering a domain name.

Government Information Technology Management[12]

The growing role of the Internet in the political economy of the United States has attracted increased congressional attention to government information technology management issues. Interest has been further heightened by national information infrastructure development efforts and e-government initiatives. Although wide-ranging, government information technology management issues can be characterized by three major themes: infrastructure development, resource management, and the provision of online services (e-government). Each of these likely will be revisited in the second session of the 107th Congress.

Internet Infrastructure and National Policy

Since 1995, when the Internet first came into prominence, the question of who should maintain and expand the U.S. information infrastructure has been raised by many policymakers. While the legislative and executive branches have had differences in the size and scope of specific initiatives and programs, both have generally supported efforts to enhance and develop non-commercial use of the Internet and information infrastructure. In its FY2002 budget request, the Bush Administration expressed continued support for federal efforts to support Internet research, technologies, and applications at the federal mission agencies, and the 107th Congress supported those goals in FY2002 appropriations bills.

At the Department of Commerce, the National Telecommunications and Information Administration (NTIA) provides guidelines and recommendations for domestic and global communications policy, manages the use of the electromagnetic spectrum for public broadcast, and awards grants to industry-public sector partnerships for research on new telecommunications applications and development of information infrastructure. The Technology Opportunity Program (TOP) provides matching merit-based grants to areas either underserved or not served at all by the Internet. The NTIA budget also includes the continued development and construction of public broadcast facilities, including funding for transition of broadcasting facilities to digital transmissions. Some policymakers support a stronger role for

---

[12] See also CRS Report RL30661, *Government Information Technology Management: Past and Future Issues (the Clinger-Cohen Act)*, by Jeffrey W. Seifert.

NTIA to close the divide between the nation's digital "haves" and "have-nots." They contend that NTIA's TOP grants and public facilities programs would be appropriate avenues for helping bridge this divide. For FY2002, Congress approved an NTIA budget of $73 million, with $15 million for TOP, $43.6 million for public telecommunications facilities, and $14 million for salaries

Information Technology R&D. Most federal Internet research and development is part of a large government effort to support a wide range of related scientific research and technology development. This is called the Information Technology Research and Development (IT R&D) initiative, and includes a wide range of programs, from software upgrades at federal agencies to high performance computing developments. While final appropriations for FY2002 have not yet been tabulated for the IT R&D initiative, preliminary figures show a total of $1.9 billion. The National Science Foundation continues to receive a significant portion of the IT R&D budget in FY2002, at $642.5 million. The Department of Energy IT R&D budget, which includes both civilian and defense IT efforts, is $480 million. Finally, the largest component of the federal IT R&D initiative is the High End Computing Infrastructure and Applications program. This multi-agency effort funds new high end computing research, technologies, and applications that will assist federal agencies perform their missions. For FY2002, this program will receive a total of $647.1 million.

Information Resource Management: The Role of a Federal CIO[13]

Debate over the creation of a federal Chief Information Officer (CIO) position has ebbed and flowed in Congress over the past five years. In private sector organizations with a CIO, this person serves as the senior decisionmaker providing leadership and direction for information resource development, procurement, and management with a focus on improving efficiency and the quality of services delivered. Creating a federal CIO position was originally considered in an early draft of what became the Clinger-Cohen Act in 1995 (P.L. 104-106), but the idea was dropped in favor of creating CIO positions within individual executive branch agencies. The CIO Council was later established in 1996 by Executive Order 13011 as a forum for agency CIOs and Deputy CIOs to share information and improve government information resource management practices. The mixed results of agency-level CIOs, combined with a growing interest in better managing government technology resources, brought renewed attention to creating a single federal CIO position, or a "national CIO," during the 106th Congress. In addition, the recent piecemeal efforts to move governmental functions and services online has led some observers to call for an "e-government czar" or a national CIO to coordinate these efforts.

Although there appears to be a growing bipartisan consensus regarding the need for a federal CIO, issues such as the organizational location and the scope of responsibility are still the subject of debate. The placement of the federal CIO is

---

[13] See also CRS Report 30914, *Federal Chief Information Officer (CIO): Opportunities and Challenges*, by Jeffrey W. Seifert, which is updated more frequently than this report.

perhaps the most hotly contested issue. Specifically, there is disagreement over whether the federal CIO should be placed in the Office of Management and Budget (OMB) or if a new office should be established within the White House to focus solely on information technology issues. In September 2000, the House Government Reform Committee's Subcommittee on Government Management, Information, and Technology held a hearing regarding two bills proposed by Representatives Turner and Davis earlier that summer (discussed below). Much of the testimony focused on the relationship between the proposed federal CIO and the OMB. Then-Deputy Director of Management at OMB, Sally Katzen, argued that situating oversight of information technology management within OMB's management and budgeting authority was essential for the successful budgeting and execution of information technology programs. In response, critics of this approach argued that IT programs are crucial enough to warrant autonomous management and budget authority by specialists who can devote their full energy to the success of government IT projects. Some observers suggest there are lessons to be learned from the lackluster results of the agency-level CIO provisions in the Clinger-Cohen Act. In reviews of this provision, the GAO has cited the divided attention of agency-level CIOs with multiple spheres of responsibility as an obstacle for implementing information technology management reforms. The GAO has further stated that the role of the CIO is a full-time leadership position requiring complete attention to information resource management issues.[14]

Another issue that has received less attention is the scope of responsibility of the proposed federal CIO. Specifically, questions have been raised about oversight of government information security. Some proponents suggest that the federal CIO should be empowered to develop and implement a comprehensive response to information security threats. Critics of this approach argue that individual agencies may believe they have a reduced obligation or will devote fewer resources to information security at a time when threats to information resources are climbing.

During the 106th Congress, legislation was introduced in the House calling for the establishment of a federal CIO position. One bill (H.R. 4670, Turner) would have created a federal CIO in an office outside of OMB, established a CIO Council by law rather than by executive order, and made the CIO head of the Council. A second bill (H.R. 5024, Davis) would have created a White House Office of Information Policy to be headed by a federal CIO, with a broad mandate to create federal IT policy, a staff, an authorized budget to carry out the duties of a federal CIO, and the power to coordinate and execute government-wide information security efforts. Neither bill was passed in the last Congress; however, these issues are being revisited in the 107th Congress.

On May 1, 2001, Senator Lieberman introduced S. 803, the E-Government Act of 2001. This bill was referred to the Governmental Affairs Committee, which held a hearing on the bill on July 11, 2001. Also on July 11, 2001, Representative Turner

---

[14] General Accounting Office, *Chief Information Officers: Ensuring Strong Leadership and an Effective Council*, GAO-T-AIMD-98-22, 27 October 1997. General Accounting Office, *VA Information Technology: Improvements Needed to Implement Legislative Reforms*, GAO/AIMD-98-154, 7 July 1998.

introduced an identical companion bill to S. 803, H.R. 2458, the E-Government Act of 2001. This bill was referred to the Committee on Government Reform. Among its many provisions, as originally introduced S. 803/H.R. 2458 called for the establishment of a federal CIO, to be appointed by the President and confirmed by the Senate. The federal CIO would have been in charge of a proposed Office of Information Policy and would report to the Director of OMB. S. 803/H.R. 2458 would also have established the CIO Council by law with the federal CIO as Chair.

On March 21, 2002, the Senate Governmental Affairs Committee reported S. 803 (now renamed the E-Government Act of 2002) with an amendment, and the Senate passed the bill unanimously on June 27, 2002. As amended, S. 803 now calls for the establishment of an office of Electronic Government within OMB. The new office is to be headed by a Senate-confirmed administrator, who in turn, is to assist OMB's Director, and Deputy Directory of Management, and work with the Administrator of the Office of Information and Regulatory affairs (OIRA) "in setting strategic direction for implementing electronic Government...." At this time, no additional action has been taken on the House companion bill, H.R. 2458.

Government Executive magazine reported that in a statement to the Congressional Internet Caucus on March 22, 2001, then-OMB Deputy Director Sean O'Keefe said that the Bush Administration opposes the creation of a separate federal CIO position in part because of concerns about agency accountability (see [http://www.govexec.com/dailyfed/0301/032301td.htm]). Instead, O'Keefe stated, the Bush Administration intends to recruit a deputy director of management for OMB who will be responsible for oversight of agency-level CIOs and coordinating e-government initiatives.

On June 14, 2001, OMB announced the appointment of Mark Forman to a newly created position, the Associate Director for Information Technology and E-Government.[15] According to the OMB announcement, as "the leading federal e-government executive," the new Associate Director will be responsible for the e-government fund, direct the activities of the CIO Council, and advise on the appointments of agency CIOs. The Associate Director will also "lead the development and implementation of federal information technology policy." The new position will report to the Deputy Director of Management at OMB, who in turn will be the federal CIO.

---

[15] Office of Management and Budget, "Mark Forman Named Associate Director for Information Technology and E-Government," 14 June 2001, [http://www.whitehouse.gov/omb/pubpress/2001-13.html].

Provision of Online Services (E-Government)[16]

Electronic government (e-government) is an evolving concept, meaning different things to different people. However, it has significant relevance to four important areas of governance: (1) delivery of services (government-to-citizen, or G2C); (2) providing information (also G2C); (3) facilitating the procurement of goods and services (government-to-business, or G2B, and business-to-government, or B2G); and (4) facilitating efficient exchanges within and between agencies (government-to-government, or G2G). For policymakers concerned about e-government, a central issue is developing a comprehensive but flexible strategy to coordinate the disparate e-government initiatives across the federal government. To that end the Bush Administration proposed a $20 million fund for fiscal 2002, growing to $100 million by the end of fiscal 2004, to support interagency e-government projects. Similarly, Senator Lieberman proposed a $200 million e-government fund in S. 803, the E-Government Act of 2001. Representative Turner also proposed a $200 million fund in H.R. 2458, the E-Government Act of 2001. However, the fiscal 2002 Treasury-Postal Service appropriations bill that was signed into law on November 12, 2001 provided for only $5 million for the e-government fund. For fiscal 2003, the Bush Administration has proposed a $45 million electronic government fund.

E-government initiatives vary significantly in their breadth and depth from state to state and agency to agency. So far, states such as California, Minnesota, and Utah have taken the lead in developing e-government initiatives. However, there is rapidly increasing interest and activity at the federal level as well. Perhaps the most well-known federal example is the September 2000 launch of the FirstGov web site [http://www.firstgov.gov]. FirstGov, which underwent a significant redesign in March 2002, is a web portal designed to serve as a single locus point for finding federal government information on the Internet. The FirstGov site also provides access to a variety of state and local government resources. Another example is the Social Security Administration (SSA), which has also launched a number of e-government initiatives including the option to apply for retirement insurance benefits online, request a Social Security Statement, and the ability to request a replacement Medicare card. At the Department of the Treasury, the U.S. Mint is using interactive Internet sales to expand its marketing efforts and attract younger people into coin collecting. Similarly, the General Services Administration (GSA) recently created a new website, FedBizOpps [http://www.fedbizopps.gov] to facilitate federal business opportunities online. The terrorist attacks of September 11, 2001 and the subsequent anthrax incidents may also motivate new e-government initiatives as Congress considers options to ensure the flow of information and services in the event of future domestic threats.

---

[16] See also CRS Report 30745, *Electronic Government: A Conceptual Overview*, by Harold C. Relyea, CRS Report 31088, *Electronic Government: Major Proposals and Initiatives*, by Harold C. Relyea, and CRS Report 31057, *A Primer on E-Government: Sectors, Stages, Opportunities, and Challenges of Online Governance*, by Jeffrey W. Seifert, which are updated more frequently than this report.

Pursuant to the July 18, 2001 OMB Memorandum M-01-28, an E-Government Task Force was established to create a strategy for achieving the Bush Administration's e-government goals.[17] In doing so, the Task Force identified 23 interagency initiatives designed to better integrate agency operations and information technology investments. These initiatives are grouped into five categories; government-to-citizen, government-to-government, government-to-business, internal effectiveness and efficiency, and addressing barriers to e-government success. Examples of these initiatives include an e-authentication project led by the General Services Administration (GSA) to increase the use of digital signatures, the eligibility assistance online project (also referred to as GovBenefits.gov) led by the Department of Labor to create a common access point for information regarding government benefits available to citizens, and the Small Business Administration's One-Stop Business Compliance project, being designed to help businesses navigate legal and regulatory requirements. A 24th initiative, a government wide payroll process project, was subsequently added.

The movement to put government online raises as many issues as it provides new opportunities. Some of these issues include, but are not limited to: security, privacy, management of governmental technology resources, accessibility of government services (including "digital divide" concerns as a result of a lack of skills or access to computers, discussed earlier), and preservation of public information (maintaining comparable freedom of information procedures for digital documents as exist for paper documents). Although these issues are neither new nor unique to e-government, they do present the challenge of performing governance functions online without sacrificing the accountability of or public access to government that citizens have grown to expect. Some industry groups have also raised concerns about the U.S. government becoming a publicly funded market competitor through the provision of fee-for-services such as the U.S. Postal Service's eBillPay, which allows consumers to schedule and make payments to creditors online [http://www.usps.com/ebpp/welcome.htm].

---

[17] See [http://www.whitehouse.gov/omb/inforeg/egovstrategy.pdf].

Appendix A: Legislation Pending in the 107th Congress

Following is a topical list of legislation pending before the 107th Congress on the issues covered in this report. The status of the legislation is not provided. For information on legislative status, congressional readers should consult LIS or Thomas, or contact CRS.

Format: Bill Number, Sponsor, Title, Date Introduced, Committee(s) to Which Bill Was Referred

Internet Privacy

H.R. 89, Frelinghuysen, Online Privacy Protection Act, 1/3/01 (Energy & Commerce)
H.R. 91, Frelinghuysen, Social Security Online Privacy Protection Act, 1/3/01 (Energy & Commerce)
H.R. 112, Holt, Electronic Privacy Protection Act, 1/3/01 (Energy & Commerce)
H.R. 220, Paul, Identity Theft Prevention Act, 1/3/01 (Ways & Means, Government Reform)
H.R. 237, Eshoo, Consumer Internet Privacy Enhancement Act, 1/20/01 (Energy & Commerce)
H.R. 333, Gekas, Bankruptcy Reform Act, 1/31/01 (Judiciary)
H.R. 347, Green, Consumer Online Privacy and Disclosure Act, 1/31/01 (Energy & Commerce)
H.R. 583, Hutchinson, Privacy Commission Act, 2/13/01 (Government Reform)
H.R. 1478, Kleczka, Personal Information Privacy Act, 4/4/01 (Ways & Means, Financial Services)
H.R. 2036, Shaw, Social Security Number Privacy and Identity Theft Prevention Act, 5/25/01 (Ways & Means, Energy & Commerce, Financial Services)
H.R. 2135, Sawyer, Consumer Privacy Protection Act, 6/12/01 (Energy & Commerce)
H.R. 2215, Sensenbrenner, Department of Justice Reauthorization Act, 6/19/01 (Judiciary)
H.R. 3053, Hooley, Identity Theft Protection Act, 10/5/01 (Financial Services)
H.R. 3482, L. Smith, CyberSecurity Enhancement Act, 12/13/01 (Judiciary)
H.R. 4678, Stearns, Consumer Privacy Protection Act, 5/8/02 (Energy & Commerce, International Relations)
H.R. 5120, Istook, FY2003 Treasury-Postal Appropriations Act, 7/15/02 (Appropriations)

S. 197, Edwards, Spyware Control and Privacy Protection Act, 1/30/01 (Commerce)
S. 420, Grassley, Bankruptcy Reform Act, 3/1/01 (Judiciary)
S. 803, Lieberman, E-Government Act, 5/1/01 (Governmental Affairs)
S. 848, Feinstein, Social Security Number Misuse Prevention Act, 5/9/01 (Judiciary)
S. 851, Thompson, Citizen's Privacy Commission Act, 5/9/01 (Governmental Affairs)
S. 1014, Bunning, Social Security Number Privacy and Identity Theft Protection Act, 6/12/01 (Finance)

S. 1055, Feinstein, Privacy Act of 2001, 6/14/01 (Judiciary)
S. 1319, Leahy, Department of Justice Authorization Act, 8/2/01 (Judiciary)
S. 1399, Feinstein, Identity Theft Protection Act, 9/4/01 (Banking)
S. 1742, Cantwell, Restore Your Identity Act, 11/29/01 (Judiciary)
S. 2201, Hollings, Online Personal Privacy Act, 4/18/02 (Judiciary)
S. 2541, Feinstein, Identity Theft Penalty Enhancement Act, 5/22/02 (Judiciary)
S. 2629, Torricelli, Federal Privacy and Data Protection Policy Act, 6/17/02 (Governmental Affairs)
S. 2839, Cleland, Children's Electronic Access Safety Enhancement (CEASE) Act, 8/1/02 (Commerce)
S. 2846, Edwards, Security and Liberty Preservation Act, 8/1/02 (Judiciary)

Computer Security

H.R. 1158, Thornberry, National Homeland Security Agency Act, 3/21/01 (Government Reform)
H.R. 1259, Morella, Computer Security Enhancement Act of 2001, 3/28/01 (Science)
H.R. 1292, Skelton, Homeland Security Strategy Act of 2001, 3/29/01 (Armed Services, Transportation & Infrastructure, Judiciary, Intelligence)
H.R. 2435, Davis, Cyber Security Information Act, 7/10/01 (Government Reform, Judiciary)
H. Con. Res. 22, Saxton, Expressing the sense of Congress regarding Internet security and "cyberterrorism," 2/6/01 (Judiciary, Education & Workforce)
H.R. 3394, Boehlert, Cyber Security Research and Development Act, 12/4/01 (Science, Education & Workforce)
H.R. 3844, Davis, Federal Information Security Management Act of 2002, 3/5/02 (Government Reform, Science)
H.R. 4660, Thornberry, National Homeland Security and Combating Terrorism Act of 2002, 5/2/02 (Government Reform)
H.R. 5005, Army, Homeland Security Act of 2002, 6/24/02 (House Select Committee on Homeland Security)

S. 1456, Bennett, Critical Infrastructure Information Security Act of 2001, 9/24/01 (Governmental Affairs)
S. 1534, Lieberman, Department of National Homeland Security Act of 2001, 10/11/01 (Governmental Affairs)
S. 1900, Edwards, Cyberterrorism Preparedness Act of 2002, 1/28/02 (Commerce)
S. 1901, Edwards, Cybersecurity Research and Education Act of 2002, 1/29/02 (Health, Education, Labor & Pensions)
S. 2182, Wyden, Cyber Security Research and Development Act, 4/17/02 (Commerce)
S. 2452, Lieberman, National Homeland Security and Combating Terrorism Act of 2002, 5/2/02 (Governmental Affairs)

Broadband Internet Access

H.R. 267, English, Broadband Internet Access Act of 2001, 1/30/01 (Ways & Means)
H.R. 1415, Rangel, Technology Bond Initiative of 2001, 4/4/01 (Ways & Means)

H.R. 1416, LaFalce, Broadband Expansion Grant Initiative of 2001, 4/4/01 (Energy & Commerce)
H.R. 1542, Tauzin, Internet Freedom and Broadband Deployment Act of 2001, 4/24/01 (Energy & Commerce)
H.R. 1693, R. Hall, Science Education for the 21st Century Act, 5/3/01 (Science, Education & Workforce)
H.R. 1697, Conyers, Broadband Competition and Incentives Act of 2001, 5/3/01 (Judiciary, Energy & Commerce)
H.R. 1698, Cannon, American Broadband Competition Act of 2001, 5/3/01 (Judiciary, Energy & Commerce)
H.R. 2038, Stupak, Rural Broadband Enhancement Act of 2001, 5/25/01 (Energy & Commerce, Agriculture)
H.R. 2120, Cannon, Broadband Antitrust Restoration and Reform Act, 6/12/01 (Judiciary, Energy & Commerce)
H.R. 2139, Smith, Rural America Broadband Deployment Act, 6/12/01 (Agriculture, Energy & Commerce)
H.R. 2401, McHugh, Rural America Digital Accessibility Act, 7/17/01 (Energy & Commerce, Ways & Means, Science)
H.R. 2597, McInnis, Broadband Deployment and Telework Incentive Act, 7/23/01 (Ways & Means)
H.R. 2669, Moran, Rural Telecommunications Enhancement Act, 7/27/01 (Agriculture, Energy & Commerce)
H.R. 2847, Boswell, Rural America Technology Enhancement Act, 9/6/01 (Agriculture, Ways & Means, Energy & Commerce, Education & the Workforce)
H.R. 4641, Markey, Wireless Technology Investment and Digital Dividends Act of 2002, 5/2/02 (Energy & Commerce)

S. 88, Rockefeller, Broadband Internet Access Act of 2001, 1/22/01 (Finance)
S. 150, Kerry, Broadband Deployment Act of 2001, 1/23/01 (Finance)
S. 426, Clinton, Technology Bond Initiative of 2001, 3/1/01 (Finance)
S. 428, Clinton, Broadband Expansion Grant Initiative of 2001, 3/1/01 (Commerce)
S. 430, Clinton, Broadband Rural Research Investment Act of 2001, 3/1/01 (Finance)
S. 966, Dorgan, Rural Broadband Enhancement Act of 2001, 5/25/01 (Commerce)
S. 1126, Brownback, Broadband Deployment and Competition Enhancement Act, 6/28/01 (Commerce)
S. 1127, Brownback, Rural Broadband Deployment Act, 6/28/01 (Commerce)
S. 1571, Lugar, Farm and Ranch Equity Act, 10/18/01 (Agriculture)
S. 1731, Harkin, Agriculture, Conservation, and Rural Enhancement Act, 11/27/01 (Agriculture)
S. 2430, Breaux, Broadband Regulatory Parity Act of 2002, 4/30/02 (Commerce)
S. 2448, Hollings, Broadband Telecommunications Act of 2002, 5/2/02 (Commerce)
S. 2863, McCain, Consumer Broadband Deregulation Act, 8/2/02 (Commerce, Science and Transportation)

Electronic Commerce

H.R. 89, Frelinghuysen, Online Privacy Protection Act, 1/3/01 (Energy & Commerce)
H.R. 1410, Istook, Internet Tax Simplification Act, 5/9/01 (Judiciary)

H.R. 1552, Cox, Internet Tax Moratorium Act, 5/9/01 (Judiciary)
H.R. 1675, Cox, Permanent Internet Tax Moratorium Act (Judiciary)

S. 288, Wyden, Internet Tax Moratorium Act, 2/8/01 (Commerce)
S. 512, Dorgan, Internet Tax Simplification Act, 3/9/01 (Finance)
S. 777, Allen, Permanent Internet Tax Moratorium Act (Commerce)

Junk E-Mail

H.R. 95, G. Green, Unsolicited Commercial Electronic Mail Act, 1/3/01 (Energy & Commerce, Judiciary)
H.R. 718, Wilson, Unsolicited Commercial Electronic Mail Act, 2/14/01 (Energy & Commerce, Judiciary)
H.R. 1017, Goodlatte, Anti-Spamming Act, 3/14/01 (Judiciary)
H.R. 3146, C. Smith, Netizens Protection Act, 10/16/01 (Energy & Commerce)

S. 630 (Burns), Can Spam Act, 3/27/01 (Commerce)

Internet Domain Names

H.R. 3833, Shimkus, Dot Kids Implementation and Efficiency Act of 2002, 3/4/02 (Energy & Commerce)
H.R. 4640, Coble, "to provide criminal penalties for providing false information in registering a domain name on the Internet," 5/2/02 (Judiciary)
H.R. 4658, Pence, Truth in Domain Names Act, 5/2/02 (Judiciary)

S. 2137, Landrieu, Family Privacy and Security Act of 2002, 4/16/02 (Commerce)
S. 2537, Dorgan, Dot Kids Implementation and Efficiency Act of 2002, 5/21/02 (Commerce, Science and Transportation)

Government Information Technology Management

H.R. 2458, Turner, E-Government Act of 2001, 7/11/01 (Government Reform)

S. 803, Lieberman, E-Government Act of 2001, 5/1/2001 (Governmental Affairs)

Appendix B: List of Acronyms

Alphabetically

ACEC	Advisory Commission on Electronic Commerce
B2B	Business-to-Business
B2G	Business-to-Government
BOC	Bell Operating Company
CIO	Chief Information Officer
DMA	Direct Marketing Association
DNS	Domain Name System
DOC	Department of Commerce
EU	European Union
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FTC	Federal Trade Commission
G2B	Government-to-Business
G2C	Government-to-Citizen
G2G	Government-to-Government
GAO	General Accounting Office
GSA	General Services Administration
gTLD	global Top Level Domain
ICANN	Internet Corporation for Assigned Names and Numbers
ILEC	Incumbent Local Exchange Carrier
IP	Internet Protocol
ISP	Internet Service Provider
IT	Information Technology
LATA	Local Access and Transport Area
LEC	Local Exchange Carrier
MOU	Memorandum of Understanding
NGI	Next Generation Internet
NIST	National Institute for Standards and Technology
NSI	Network Solutions, Inc,
NSF	National Science Foundation
NTIA	National Telecommunications and Information Administration
ONDCP	Office of National Drug Control Policy
OPA	Online Privacy Alliance
SSA	Social Security Administration
SSN	Social Security Number
TLD	Top Level Domain
UCE	Unsolicited Commercial E-mail
WIPO	World Intellectual Property Organization
WTO	World Trade Organization

Categorically

U.S. Government Entities

DOC	Department of Commerce
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FTC	Federal Trade Commission
GAO	General Accounting Office
GSA	Government Services Administration
NIST	National Institute of Standards and Technology (part of Department of Commerce)
NSF	National Science Foundation
NTIA	National Telecommunications and Information Administration (part of Department of Commerce)
ONDCP	Office of National Drug Control Policy
SSA	Social Security Administration

Private Sector Entities

BOC	Bell Operating Company
DMA	Direct Marketing Association
ICANN	Internet Corporation for Assigned Names and Numbers
ILEC	Incumbent Local Exchange Carrier
ISP	Internet Service Provider
LEC	Local Exchange Carrier
NSI	Network Solutions, Inc.
OPA	Online Privacy Alliance

General Types of Internet Services

B2B	Business-to-Business
B2G	Business-to-Government
G2B	Government-to-Business
G2C	Government-to-Citizen
G2G	Government-to-Government

Internet and Telecommunications Terminology

CIO	Chief Information Officer
DNS	Domain Name System
gTLD	global Top Level Domain
IP	Internet Protocol
IT	Information Technology
LATA	Local Access and Transport Area
NGI	Next Generation Internet
TLD	Top Level Domain
UCE	Unsolicited Commercial E-mail

Other

ACEC	Advisory Commission on Electronic Commerce
EU	European Union
MOU	Memorandum of Understanding
SSN	Social Security Number
WIPO	World Intellectual Property Organization
WTO	World Trade Organization

Appendix C: Legislation Passed by the 105th and 106th Congresses

Editions of this report prepared in the 105th Congress and the 106th Congress also addressed key technology policy issues affecting the use of growth of the Internet. Some of those issues continue to be of interest to Congress and are discussed in this edition of the report. Others, however, appear to be resolved from a congressional point of view, at least the moment, specifically encryption, electronic signatures, and protecting children from unsuitable material on the Internet. Those topics are not discussed in this version of the report. Nevertheless, it appears useful to retain information about legislation that passed on the subjects of most interest to the two previous Congresses. Following is such a summary, based on the topics that were previously covered in the report.

Legislation Enacted in the 105th Congress

Protecting Children: Child Online Protection Act, Children's Online Privacy Protection Act, and Child Protection and Sexual Predator Protection Act

In the FY1999 Omnibus Consolidated and Emergency Supplemental Appropriations Act (P.L. 105-277), Congress included several provisions related to protecting children on the Internet. Included is legislation making it a crime to send material that is "harmful to minors" to children and protecting the privacy of information provided by children under 13 over interactive computer services. Separately, Congress passed a law (P.L. 105-314) that, *inter alia*, strengthens penalties against sexual predators using the Internet.

The "harmful to minors" language is in the **Child Online Protection Act**, Title XIV of Division C of the Omnibus Appropriations Act. Similar language was also included in the Internet Tax Freedom Act (Title XI of Division C of the Omnibus Appropriations Act). Called "CDA II" by some in reference to the Communications Decency Act that passed Congress in 1996 but was overturned by the Supreme Court, the bill restricts access to commercial material that is "harmful to minors" distributed on the World Wide Web to those 17 and older. The American Civil Liberties Union (ACLU) and others filed suit against enforcement of the portion of the Act dealing with the "harmful to minors" language. In February, 1999, a federal judge in Philadelphia issued a preliminary injunction against enforcement of that section of the Act. The Justice Department has filed an appeal (see CRS Report 98-670, *Obscenity, Child Pornography, and Indecency: Recent Developments and Pending Issues* for further information).

The **Children's Online Privacy Protection Act**, also part of the Omnibus Appropriations Act (Title XIII of Division C), requires verifiable parental consent for the collection, use, or dissemination of personally identifiable information from children under 13.

The Omnibus Appropriation Act also includes a provision intended to make it easier for the FBI to gain access to Internet service provider records of suspected sexual predators (Section 102, General Provisions, Justice Department). It also sets

aside $2.4 million for the Customs Service to double the staffing and resources for the child pornography cyber-smuggling initiative and provides $1 million in the Violent Crime Reduction Trust Fund for technology support for that initiative.

The **Protection of Children from Sexual Predators Act** (P.L. 105-314) is a broad law addressing concerns about sexual predators. Among its provisions are increased penalties for anyone who uses a computer to persuade, entice, coerce, or facilitate the transport of a child to engage in prohibited sexual activity, a requirement that Internet service providers report to law enforcement if they become aware of child pornography activities, a requirement that federal prisoners using the Internet be supervised, and a requirement for a study by the National Academy of Sciences on how to reduce the availability to children of pornography on the Internet.

Identity Theft and Assumption Deterrence Act

The Identity Theft and Assumption Deterrence Act (P.L. 105-318) sets penalties for persons who knowingly, and with the intent to commit unlawful activities, possess, transfer, or use one or more means of identification not legally issued for use to that person.

Intellectual Property: Digital Millennium Copyright Act

Congress passed legislation (P.L. 105-304) implementing the World Intellectual Property Organization (WIPO) treaties regarding protection of copyright on the Internet. The law also limits copyright infringement liability for online service providers that serve only as conduits of information. Provisions relating to database protection that were included by the House were not included in the enacted version and are being debated anew in the 106th Congress. Since database protection per se is not an Internet issue, it is not included in this report (see CRS Report 98-902, *Intellectual Property Protection for Noncreative Databases*).

Digital Signatures: Government Paperwork Elimination Act

Congress passed the Government Paperwork Elimination Act (Title XVII of Division C of the Omnibus Appropriations Act, P.L. 105-277) that directs the Office of Management and Budget to develop procedures for the use and acceptance of "electronic" signatures (of which digital signatures are one type) by executive branch agencies.

Internet Domain Names: Next Generation Internet Research Act

The Next Generation Internet Research Act (P.L. 105-305) directs the National Academy of Sciences to conduct a study of the short and long-term effects on trademark rights of adding new generation top-level domains and related dispute resolution procedures.

Summary of Legislation Passed by the 105th Congress

Title	Public Law Number
FY1999 Omnibus Consolidated and Emergency Supplemental Appropriations Act	**P.L. 105-277**
Internet Tax Freedom Act	Division C, Title XI
Children's Online Privacy Protection Act	Division C, Title XIII
Child Online Protection Act	Division C, Title XIV
Government Paperwork Elimination Act	Division C, Title XVII
Protection of Children from Sexual Predators Act	**P.L. 105-314**
Identity Theft and Assumption Deterrence Act	**P.L. 105-318**
Digital Millennium Copyright Act	**P.L. 105-304**
Next Generation Internet Research Act	**P.L. 105-305**

Legislation Enacted in the 106th Congress

Electronic Signatures

The **Millennium Digital Commerce Act (P.L. 106-229)** regulates Internet electronic commerce by permitting and encouraging its continued expansion through the operation of free market forces, including the legal recognition of electronic signatures and electronic records.

Computer Security

The **Computer Crime Enforcement Act (P.L. 106-572)** establishes Department of Justice grants to state and local authorities to help them investigate and prosecute computer crimes. The law authorizes the expenditure of $25 million for the grant program through FY2004. The **FY2001 Department of Defense Authorization Act (P.L. 106-398)** includes language that originated in S. 1993 to modify the Paperwork Reduction Act and other relevant statutes concerning computer security of government systems, codifying agency responsibilities regarding computer security.

Internet Privacy

Language in the **FY2001 Transportation Appropriations Act (P. L. 106-246)** and the **FY2001 Treasury-General Government Appropriations Act** (included as part of the Consolidated Appropriations Act, P.L. 106-554) addresses Web site information collection practices by departments and agencies in the Treasury-General Government Appropriations Act. Section 501 of the FY2001 Transportation Appropriations Act prohibits funds in the FY2001 Treasury-General Government Appropriations Act from being used by any federal agency to collect, review, or create aggregate lists that include personally identifiable information (PII) about an individual's access to or use of a federal Web site, or enter into agreements with third parties to do so, with exceptions. Section 646 of the FY2001 Treasury-General Government Appropriations Act requires Inspectors General of agencies or departments covered in that act to report to Congress within 60 days of enactment on activities by those agencies or departments relating to the collection of PII about individuals who access any Internet site of that department or agency, or entering into agreements with third parties to obtain PII about use of government or non-government Web sites.

The **Social Security Number Confidentiality Act (P.L. 106-433)** prohibits the display of Social Security numbers on unopened checks or other Treasury-issued drafts. (Although this is not an Internet issue, it is related to concerns about consumer identity theft, a topic addressed in this report.)

The **Internet False Identification Prevention Act (P.L. 106-578)** updates existing law against selling or distributing false identification documents to include those sold or distributed through computer files, templates, and disks. It also requires the Attorney General and Secretary of the Treasury to create a coordinating committee to ensure that the creation and distribution of false IDs is vigorously investigated and prosecuted.

Protecting Children from Unsuitable Material

The **Children's Internet Protection Act (Title XVII of the FY2001 Labor-HHS Appropriations Act, included in the FY2001 Consolidated Appropriations Act, P.L. 106-554)** requires most schools and libraries that receive federal funding through Title III of the Elementary and Secondary Education Act, the Museum and Library Services Act, or "E-rate" subsidies from the universal service fund, to use technology protection measures (filtering software or other technologies) to block certain Web sites when computers are being used by minors, and in some cases, by adults. When minors are using the computers, the technology protection measure must block access to visual depictions that are obscene, child pornography, or harmful to minors. When others are using the computers, the technology must block visual depictions that are obscene or are child pornography. The technology protection measure may be disabled by authorized persons to enable access for bona fide research or other lawful purposes.

Internet Domain Names

The **Anticybersquatting Consumer Protection Act (part of the FY2000 Consolidated Appropriations Act, P.L. 106-113)** gives courts the authority to order the forfeiture, cancellation, and/or transfer of domain names registered in "bad faith" that are identical or similar to trademarks. The Act provides for statutory civil damages of at least $1,000, but not more than $100,000 per domain name identifier.

Summary of Legislation Enacted in the 106th Congress

Title	Public Law Number
Millennium Digital Commerce Act	**P.L. 106-229**
Computer Crime Enforcement Act	**P.L. 106-572**
FY2001 Transportation Appropriations Act, section 501	**P.L. 106-246**
FY2001 Treasury-General Government Appropriations Act, section 646 (enacted by reference in the FY2001 Consolidated Appropriations Act)	**P.L. 106-554**
Social Security Number Confidentiality Act	**P.L. 106-433**
Internet False Identification Prevention Act	**P.L. 106-578**
Children's Internet Protection Act (Title XVII of the FY2001 Labor-HHS Appropriations Act, enacted by reference in the FY2001 Consolidated Appropriations Act)	**P.L. 106-554**
Anticybersquatting Consumer Protection Act (enacted by reference in the FY2000 Consolidated Appropriations Act)	**P.L. 106-113**

Appendix D: Related CRS Reports

Internet Privacy

CRS Report RL30677. *Digital Surveillance: the Communications Assistance for Law Enforcement Act and FBI Internet Monitoring*, by Richard M. Nunno.

CRS Report RL31289. *The Internet and the USA PATRIOT Act: Potential Implications for Electronic Privacy, Security, Commerce, and Government*, by Marcia S. Smith, Jeffrey W. Seifert, Glenn J. McLoughlin, and John Dimitri Moteff.

CRS Report RL30784. *Internet Privacy: An Analysis of Technology and Policy Issues*, by Marcia S. Smith.

CRS Report RL31408. *Internet Privacy: Overview and Pending Legislation*, by Marcia S. Smith.

CRS Report RL30322. *Online Privacy Protection: Issues and Developments*, by Gina Marie Stevens.

CRS Report RL30671. *Personal Privacy Protection: The Legislative Response*, by Harold C. Relyea.

CRS Report 98-326. *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, by Gina Marie Stevens and Charles Doyle.

CRS Report RS21221. *Privacy Protection for Online Information*, by Gina Marie Stevens.

CRS Report RL31200. *Terrorism: Section by Section Analysis of the USA PATRIOT Act*, by Charles Doyle.

CRS Report RL31377. *The USA PATRIOT Act: A Legal Analysis*, by Charles Doyle.

CRS Report RS21203. *The USA PATRIOT Act: A Sketch*, by Charles Doyle.

Computer Security

CRS Report RL30153. *Critical Infrastructures: Background and Early Implementation of PDD-63*, by John D. Moteff.

CRS Report RL31289. *The Internet and the USA PATRIOT Act: Potential Implications for Electronic Privacy, Security, Commerce, and Government*, by Marcia S. Smith, Jeffrey W. Seifert, Glenn J. McLoughlin, and John Dimitri Moteff.

Broadband Internet Access

CRS Issue Brief IB10045. *Broadband Internet Access: Background and Issues*, by Angele A. Gilroy and Lennard G. Kruger.

CRS Report RL30719. *Broadband Internet Access and the Digital Divide: Federal Assistance Programs*, by Lennard G. Kruger.

CRS Report RL30018. *Long Distance Telephony: Bell Operating Company Entry Into the Long Distance Market*, by James R. Riehl.

CRS Issue Brief IB98040. *Telecommunications Discounts for Schools and Libraries: the "E-Rate" Program and Controversies*, by Angele Gilroy.

Electronic Commerce

CRS Report RL31293. *E-Commerce Statistics: Explanation and Sources*, by Rita E. Tehan.

CRS Report RS20426. *Electronic Commerce: An Introduction*, by Glenn J. McLoughlin.

CRS Report RS20344. *Electronic Signatures: Technology Developments and Legislative Issues*, by Richard Nunno.

CRS Report RL31177. *Extending the Internet Tax Moratorium and Related Issues*, by Nonna A. Noto.

CRS Report RL31158. *Internet Tax Bills in the 107th Congress: A Brief Comparison*, by Nonna A. Noto.

IP539P. *Electronic Commerce, Info Pack*, by Rita Tehan.

CRS Report RL31289. *The Internet and the USA PATRIOT Act: Potential Implications for Electronic Privacy, Security, Commerce, and Government*, by Marcia S. Smith, Jeffrey W. Seifert, Glenn J. McLoughlin, and John Dimitri Moteff.

CRS Report RL31252, *Internet Commerce and State Sales and Use Taxes*, by Stephen Maguire.

CRS Report RS20577. *State Sales Taxation of Internet Transactions*, by John Luckey.

Unsolicited Commercial Electronic Mail (Junk E-Mail or Spam)

CRS Report RS20037. *"Junk E-mail": An Overview of Issues and Legislation Concerning Unsolicited Commercial Electronic Mail ("Spam")*, by Marcia S. Smith.

CRS Report RL30763. *Telemarketing: Dealing with Unwanted Telemarketing Calls*, by James R. Riehl.

Internet Domain Names

CRS Report 97-868 STM. *Internet Domain Names: Background and Policy Issues*, by Lennard G. Kruger.

Government Information Technology Management

CRS Report RS21140. *Electronic Congress: Proposals and Issues*, by Jeffrey W. Seifert and R. Eric Petersen.

CRS Report RL30745. *Electronic Government: A Conceptual Overview*, by Harold C. Relyea.

CRS Report RL30914. *Federal Chief Information Officer (CIO): Opportunities and Challenges*, by Jeffrey W. Seifert.

CRS Report RL30661. *Government Information Technology Management: Past and Future Issues (the Clinger-Cohen Act)*, by Jeffrey W. Seifert.

CRS Report RL31103. *House of Representatives Information Technology Management Issues: An Overview of the Effects on Institutional Operations, the Legislative Process, and Future Planning*, by Jeffrey W. Seifert and R. Eric Petersen. 21 p.

CRS Report RL31289. *The Internet and the USA PATRIOT Act: Potential Implications for Electronic Privacy, Security, Commerce, and Government*, by Marcia S. Smith, Jeffrey W. Seifert, Glenn J. McLoughlin, and John Dimitri Moteff.

CRS Report RL31057. *A Primer on E-Government: Sectors, Stages, Opportunities, and Challenges of Online Governance*, by Jeffrey W. Seifert.

Related Topics

Computer Fraud and Abuse

CRS Report RS20830. *Computer Fraud and Abuse: A Sketch of 18 U.S.C. 1030 and Related Federal Criminal Laws*, by Charles Doyle.

CRS Report 97-1025 A. *Computer Fraud & Abuse: An Overview of 18 U.S.C. 1030 And Related Federal Criminal Laws*, by Charles Doyle.

Copyright and "Fair Use"

CRS Report RL30683. *Copyright Cases in the Courts: Napster, MP3 Digital Music, and DVD Motion Picture Encryption Technology*, by Robin Jeweler.

CRS Report RL31029. *Copyright Issues in Online Music Delivery*, by Robin Jeweler.

CRS Report RL31423. *Fair Use on the Internet*, by Christopher A. Jennings.

CRS Report RS21206. *"Fair Use" on the Internet: Linking, Framing, and Copyright's Reproduction and Public Display Rights*, by Christopher A. Jennings.

Internet-General

CRS Report RL31270. *Internet Statistics: Explanation and Sources*, by Rita E. Tehan.

CRS Report RL30987. *Spinning the Web: the Internet's History and Structure*, by Rita Tehan.

Medical Records, Financial, and Other Privacy Issues

CRS Report RS20934. *Brief Summary of the Medical Privacy Rule*, by Gina Marie Stevens.

CRS Report RL30620. *Health Information Security and Privacy: HIPAA and Proposed Implementing Regulations*, by C. Stephen Redhead.

CRS Report RS20500. *Medical Records Privacy: Questions and Answers on the December 2000 Federal Regulation*, by C. Stephen Redhead.

CRS Report RS20185. *Privacy Protection for Customer Financial Information*, by M. Maureen Murphy.

Protecting Children

CRS Report RS20036. *Internet—Protecting Children from Unsuitable Material and Sexual Predators: Overview and Pending Legislation*, by Marcia S. Smith.

CRS Report 98-670 A. *Obscenity, Child Pornography, and Indecency: Recent Developments and Pending Issues*, by Henry Cohen.

Other Related Topics

CRS Report RL30602. *Electronic Stock Market*, by Mark Jickling.

CRS Report 97-619 A. *Internet Gambling: Overview of Federal Criminal Law*, by Charles Doyle.

CRS Report RS20639. *Internet Voting: Issues and Legislation*, by Kevin Coleman.

CRS Report RL30456. *Prescription Drug Sales Over the Internet*, by Christopher Sroka.

CRS Report RL30863. *Telework in the Federal Government: Background, Policy, and Oversight*, by Lorraine H. Tong and Barbara L. Schwemle.