Order Code 98-67 STM

CRS Report for Congress
Received through the CRS Web

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

Updated December 29, 2004

Marcia S. Smith, John D. Moteff, Lennard G. Kruger,
Glenn J. McLoughlin, Jeffrey W. Seifert,
and Patricia Moloney Figliola
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 Congress. This report summarizes several key technology policy issues.

1. **Internet privacy** issues encompass concerns about information collected by website operators and by "spyware," and about the extent to which law enforcement officials are allowed to monitor an individual's Internet activities. Congress has passed several laws already, but continues to debate what other legislation may be needed.

2. Concerns about **computer and Internet security** are prevalent in both the government and private sectors. Issues have also been raised about the vulnerability of the nation's critical infrastructures (e.g. electrical power supply) to cyber attacks. Issues for 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 three-year tax moratorium on domestic e-commerce taxation, the impact of the USA PATRIOT Act, and how the policies of the European Union and the World Trade Organization (WTO) may affect U.S. e-commerce activities.

5. The new federal anti-**spam** law, the CAN-SPAM Act, permits, but does not require, the Federal Trade Commission (FTC) to create a "do not e-mail" list similar to the National Do Not Call list for telemarketers. Whether to require the FTC to establish such a list, and the extent to which the new law will actually reduce the amount of spam, remain congressional issues in the wake of the law's enactment.

6. The administration and governance of the **Internet's domain name system** (DNS) is currently under transition from federal to private sector control. 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 evolving role of the Internet in the political economy of the United States continues to attract congressional attention. Among the issues are information technology research and development, the provision of online services by the government ("**e-government**"), and availability and use of "open source" software.

Contents

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, access to broadband (high-speed) services, electronic commerce (e-commerce), the impact of "spam," Internet domain names, and government information technology management. This report provides short summaries of those issues, plus appendices providing a list of acronyms, a discussion of related legislation passed in the 105th - 107th Congresses, and a list of other CRS reports that provide more detail on these topics.

Legislation Passed by the 108th Congress

The 108th Congress passed several laws related to the topics covered in this report. A brief summary of the new laws follows.

Internet Privacy: The Intelligence Reform and Terrorism Protection Act (P.L. 108-458)

The Intelligence Reform and Terrorism Protection Act (P.L. 108-458) was passed largely in response to recommendations from the 9/11 Commission, which investigated the September 11, 2001 terrorist attacks. Among its many provisions, the act creates a Privacy and Civil Liberties Oversight Board, composed of five members, two of whom (the chairman and vice-chairman) must be confirmed by the Senate. The Board's mandate is to ensure that privacy and civil liberties are not neglected when implementing terrorism-related laws, regulations, and policies. The 9/11 Commission had recommended creation of such a Board because of concern that the USA PATRIOT Act, enacted soon after the attacks, shifts the balance of power to the government.

Broadband Internet Access: Commercial Spectrum Enhancement Act (P.L. 108-494)

The Commercial Spectrum Enhancement Act (Title II of H.R. 5419, P.L. 108-494) seeks to make more spectrum available for wireless broadband and other services by facilitating the reallocation of spectrum from government to commercial users.

E-Commerce: Internet Tax Non-Discrimination Act (P.L. 108-435)

Facing the expiration of an existing moratorium on Internet taxes, the 108th Congress passed S. 150, the Internet Tax Non-Discrimination Act. President Bush signed the bill into law on December 3, 2004 (P.L. 108-435). Among its provisions, the act: 1) extended the e-commerce tax moratorium for four years, from November 1, 2003 through November 1, 2007; 2) expanded the definition of Internet access to include both providers and buyers of Internet access; 3) grandfathered through November 1, 2007, Internet access taxes enforced before October 1, 1998; 4) similarly grandfathered through November 1, 2005 Internet access taxes enforced before November 1, 2003; and 5) excluded Voice Over Internet Protocol (VoIP) and similar voice services.

Spam: The CAN-SPAM Act (P.L. 108-187)

P.L. 108-187 (S. 877), **the CAN-SPAM Act**, sets civil or criminal penalties if senders of commercial e-mail do not provide a legitimate opportunity for recipients to "opt-out" of receiving further commercial e-mail from the sender, if they use deceptive subject headings, if they use fraudulent information in the header of the message, if they "harvest" e-mail addresses from the Internet or use "dictionary attacks" to create e-mail addresses, if they access someone else's computer without authorization and use it to send multiple commercial e-mail messages, or engage in certain other activities connected with sending "spam." Spam is variously defined by participants in the debate as unsolicited commercial e-mail, unwanted commercial e-mail, or fraudulent commercial e-mail. The CAN-SPAM Act preempts state laws that specifically regulate electronic mail, but not other state laws, such as trespass, contract, or tort law, or other state laws to the extent they relate to fraud or computer crime. It authorizes, but does not require, the Federal Trade Commission to establish a centralized "do not e-mail" list similar to the National Do Not Call list for telemarketing. The FTC has concluded that a do not e-mail list is not feasible at this time.

Domain Names: The PROTECT Act (P.L. 108-21), and The Fraudulent Online Identity Sanctions Act (P.L. 108-482)

P.L. 108-21 (S. 151), **the PROTECT Act**, contains a provision (Sec. 108, Misleading Domain Names on the Internet) that makes it a punishable crime to knowingly use a misleading domain name with the intent to deceive a person into viewing obscenity on the Internet. Increased penalties are provided for deceiving minors into viewing harmful material. (CRS Report RS21328 provides further information on this and other legislative efforts to protect children from unsuitable material on the Internet.)

The **Fraudulent Online Identity Sanctions Act** was incorporated as Title II of H.R. 3632, the Intellectual Property Protection and Courts Amendments Act of 2004 (P.L. 108-482). The act increases criminal penalties for those who submit false contact information when registering a domain name that is subsequently used to commit a crime or engage in copyright or trademark infringement.

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 website operators collect personally identifiable information (PII) about visitors to their websites 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 websites are monitored by government or law enforcement officials, employers, or e-mail service providers. "Spyware," generally defined as software that is loaded onto a user's computer without his or her knowledge, also is arousing considerable attention. Some spyware tracks the user's activities and reports back to a third party, changes computer settings, or takes control of their computer's browser.

Collection of Data by Website Operators and Fair Information Practices

One aspect of the Internet privacy issue is whether commercial websites 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. Some add *enforcement* as a fifth practice. 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 websites 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 Websites. Based on surveys of commercial websites between 1997 and 2000, the FTC 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 website 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. (On June 11, 2003, the chairman of the FTC told the Senate Commerce Committee that the FTC had brought eight COPPA cases, and obtained agreements requiring payment of civil penalties totaling more than $350,000.)

---

[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.

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 website operators to follow the four fair information practices. In June 2001, Timothy Muris succeeded Robert Pitofsky as FTC chairman, and later indicated that he did not see a need for additional legislation at that time. (Mr. Muris since has been succeeded by Deborah Platt Majoras.)

The Internet industry has taken steps to demonstrate that it can self regulate. One example is the establishment of "seals" for websites by the Better Business Bureau, TRUSTe, and WebTrust. To display a seal from one of those organizations, a website operator must agree to abide by certain privacy principles, a complaint resolution process, and to being monitored for compliance. Another approach is using software called "P3P" (Platform for Privacy Preferences Project) 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. Some also consider P3P to be insufficient.

A number of bills were introduced in the 108th Congress regarding commercial website privacy, but none passed.

Federal Websites. Until the summer of 2000, attention was focused on privacy issues associated with commercial websites. That changed in June 2000, however, when controversy erupted over the privacy of visitors to government websites. The issue concerned federal agencies' use of computer "cookies"(small text files placed on users' computers when they access a particular website) to track activity at their websites. 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, it became known that contractors for the Office of National Drug Control Policy (ONDCP) were using cookies to collect information about those using ONDCP's website during an anti-drug campaign. 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 passed a provision in the FY2001 Treasury-General Government Appropriations Act (the "Treasury-Postal" Appropriations Act) and the FY2001 Transportation Appropriations Act (P.L. 106-346, Section 501) that prohibited funds

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 website or enter into agreements with third parties to do so, with exceptions. Similar language has been included in subsequent appropriations acts, most recently the Treasury-Transportation section of the FY2005 Consolidated Appropriations Act (P.L. 108-447). Congress also passed the E-Government Act (P.L. 107-347) which requires federal websites to include a privacy notice that addresses what information is to be collected, why, its intended use, what notice or opportunities for consent are available to individuals regarding what is collected and how it is shared, how the information will be secured, and the rights of individuals under the 1974 Privacy Act and other relevant laws. It also requires federal websites to translate their privacy policies into a standardized machine-readable format, enabling P3P to work, for example.

Monitoring of E-Mail and Web Activity

By Government and Law Enforcement Officials. Another Internet privacy storm broke in the summer of 2000 when it became known that the FBI, with a court order, can install 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 (later renamed "DCS 1000"), could differentiate between e-mail and Web activity involving a subject of an FBI investigation and other people's e-mail and Web activity was of considerable debate, with critics claiming that Carnivore violated the privacy of innocent users. The 21st Century Department of Justice Authorization Act (P.L. 107-273) required the Justice Department to report to Congress on its use of DCS 1000 or any similar system at the end of FY2002 and FY2003.

However, following the September 11, 2001, terrorist attacks, Congress also passed the USA PATRIOT Act (P.L. 107-56), which expands law enforcement's ability to monitor Internet activities. The Internet privacy-related provisions of the USA PATRIOT Act are discussed in CRS Report RL31289. One of the controversial provisions is Section 212. As originally enacted, that section 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. In 2002, Congress amended this section, lowering the threshold for when ISPs could voluntarily divulge information, and to whom. Under the Cyber Security Enhancement Act, section 225 of the Homeland Security Act (P.L. 107-296), ISPs need only a "good faith" belief (instead of a "reasonable" belief), that there is an emergency involving danger (instead of "immediate" danger) of death or serious physical injury. The contents of the communication can be disclosed to "a Federal, state, or local governmental entity" (instead of a "law enforcement agency").

Privacy advocates complain that it is extremely difficult to monitor how the USA PATRIOT Act is being implemented. They are especially concerned about the amendment made by the Cyber Security Enhancement Act. For example, the Electronic Privacy Information Center (EPIC) notes that allowing such information to be disclosed to any governmental entity not only poses increased risk to personal privacy, but also is a poor security strategy; and that the language does not provide for judicial oversight of the use of these procedures.

Several of the Internet-related sections of the USA PATRIOT Act, including Sec. 212, are covered by a "sunset" provision under which they will expire on December 31, 2005. Three bills were introduced in the 108th Congress that would either have extended the sunset clause to additional sections, or abolished the sunset clause entirely so that none of the provisions would expire. None of those bills passed. For more on the sunset clause, see CRS Report RL32186.

By Employers. An emerging issue is whether employers should be required to notify their employees if e-mail or other computer-based activities are monitored. A 2003 survey by the American Management Association [http://www.amanet.org/research/index.htm] found that 52% of the companies surveyed engage in some form of e-mail monitoring. 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.

By E-Mail Service Providers. In what is widely-regarded as a landmark ruling concerning Internet privacy, the U.S. Court of Appeals for the First Circuit in Massachusetts ruled (2-1) on June 29, 2004, that an e-mail service provider did not violate the Wiretap Act (18 U.S.C. §§ 2510-2522) when it intercepted and read subscribers' e-mails to obtain a competitive business advantage. The case involved Bradford Councilman, a Vice President of Interloc, Inc., an e-mail service provider that sold out-of-print books. Interloc used software to intercept and copy e-mail messages sent to its subscribers (who were dealers looking for buyers of rare and out-of-print books) by competitor Amazon.com so that Interloc officials could read the e-mails and obtain a competitive advantage over Amazon.com. The case turned on the distinction between the e-mail being in transit, or in storage (and therefore governed by a different law, the Stored Communications Act, 18 U.S.C. §§ 2701-2711). Privacy advocates expressed deep concern about the ruling. The Department of Justice is appealing the case. Two bills were introduced in the 108th Congress that would have affected this debate by amending either the Wiretap Act (H.R. 4977) or the Stored Communications Act (H.R. 5059). There was no action on either bill.

Spyware

The term "spyware" is not well defined. One example of spyware is software products that 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. Some products may collect personally identifiable information (PII). When the computer is connected to the Internet, the software periodically relays the information back to the software manufacturer or a marketing company. Some spyware traces a user's Web activity and causes advertisements to suddenly appear on the user's monitor — called "pop-up" ads — in response. Such software is called "adware." Software

programs that include spyware can be sold or provided for free, on a disk (or other media) or downloaded from the Internet. Typically, users have no knowledge that spyware is on their computers.

A central point of the debate is whether new laws are needed, or if industry self-regulation, coupled with enforcement actions under existing laws such as the Federal Trade Commission Act, is sufficient. The lack of a precise definition for spyware is cited as a fundamental problem in attempting to write new laws. FTC representatives and others caution that new legislation could have unintended consequences, barring current or future technologies that might, in fact, have beneficial uses. They further insist that, if legal action is necessary, existing laws provide sufficient authority. Consumer concern about control of their computers being taken over by spyware leads others to conclude that legislative action is needed.

Utah and California have passed spyware laws, but there is no specific federal law regarding spyware. In the 108th Congress, the House passed two bills (H.R. 2929 and H.R. 4661) and the Senate Commerce Committee reported S. 2145. There was no further action. Debate is likely to resume in the 109th Congress.

Computer and Internet Security

On October 21, 2002, all 13 of the Internet's root Domain Name System servers were targeted by a distributed denial of service attack. While the attack had little overall effect on the performance of the Internet, a more sophisticated and sustainable attack might have had a more deleterious impact. As use of the Internet grows, so has concern about security of and security on the Internet. A long list of security-related incidents that have received wide-ranging media coverage (e.g. the Melissa virus, the Love Bug, and the Code Red, Code Red II, Nimda, Slammer and Blaster 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 do not 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 over 137,000 incidents in 2003. Since many attacks are now coordinated and cascade throughout the Internet, CERT no longer tracks the number of incidents

reported to them. While the total number of incidents may be rising exponentially, it is interesting to note that, according to the Computer Crime and Security Survey, the percentage of respondents that reported unauthorized use of their computer systems over the last 12 months has steadily declined over the last four years.[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 are largely speculative. 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. In the 2004 Computer Crime and Security Survey, 269 responders (out of a total of 494) estimated financial losses of $141 million in the previous 12 months. The 2004 survey found for the first time that those reporting losses attributed them to viruses and denial of service attacks, versus the loss of proprietary information and fraud, which had been identified as the the primary cause for losses in previous surveys. For more discussion on the economic impact of attacks against computer systems, and the difficulties in measuring it, see CRS Report RL32331, *The Economic Impact of Cyber-Attacks*.

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. In February 2003, the President's Critical Infrastructure Board (established by President George W. Bush through E.O. 13231 but later dissolved by E.O. 13286) released a *National Strategy to Secure Cyberspace*. This latter *Strategy* assigned a number of

---

[2] The Computer Crime and Security Survey is conducted by the Computer Security Institute (CSI) in cooperation with the San Francisco Federal Bureau of Investigation's Computer Intrusion Squad. The CSI/FBI Survey, as it has become known, has been conducted annually since 1996, and surveys U.S. corporations, government agencies, financial and medical institutions and universities. The Survey does not discuss the reasons for this decline; i.e. whether it is do improved security, non-reporting, attacks that go unnoticed, or fewer attacks. The CSI/FBI survey does not represent a statistical sampling of the nation's computer security practitioners. The survey can be found at [http://www.gocsi.com] . This website was last viewed on Nov. 17, 2004. A newer survey conducted by CERT, the U.S. Secret Service and the CSO Magazine (*2004 E-Crime Watch Survey)* reported that 43% of its respondents reported an increase in e-crimes or intrusions committed against their organization. E-crimes include any crime in which electronic media has been used in its commission. The unit of measure in these two surveys are not the same.

responsibilities for coordinating the protection of the nation's information infrastructure to the new Department of Homeland Security. Most of the Department's efforts in cybersecurity are directed by the National Cyber Security Division within the Information Analysis and Infrastructure Protection Directorate.

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, 2001 terrorist attacks, increased some of the penalties associated with these illegal activities. The USA PATRIOT Act also permits a single warrant to be granted to allow investigators to track hackers across jurisdictions. The Homeland Security Act (P.L. 107-296) increased penalties for anyone who knowingly or recklessly causes injury or death, while knowingly transmitting malicious code or commands.

At the international level, the 41-country Council of Europe negotiated a convention to facilitate tracking cyber criminals across national boundaries.[3] The United States, an observer at these negotiations, signed the convention and is encouraging other countries to do so, too. U.S. businesses had expressed some concern about their liability and the costs associated with record-keeping under this treaty. In addition to this forum, the European Commission has published a couple of communiques related to network security and the Organization of Economic Cooperation and Development has reissued a set of guidelines related to information and network security. There is also some debate within the international community on what to do about computer intrusions by government agents; for example, whether such acts would be considered acts of war.

The federal government is required to protect sensitive information on its own computers. Congress passed the most recent requirements for federal agencies to follow in the Federal Information Security Management Act of 2002 (P.L. 107-347, Title III). These include following guidelines developed by the National Institute of Standards and Technology. and Office of Management and Budget (OMB) Circular A-130, Appendix III, in developing agency-wide information security programs. The Federal Information Security Management Act (FISMA) also requires agencies to submit their information security programs to an annual independent evaluation, the results of which are summarized and reported to Congress.

---

[3] The Convention on Cybercrime, ETS-185 can be found on the Council's web page, at [http://conventions.coe.int]; click on Full List of European Treaties. This web page was last viewed on Dec. 23, 2003.

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. The market for computer and Internet security (divided into hardware, software, and service providers) is large and growing. PCWorld.com reported that an International Data Corporation (IDC) study estimated that the world network security market will grow from $17 billion in 2001 to $45 billion by 2006.[4] According to the CSI/FBI report, roughly half of those organizations that responded spend between 1% and 5% of their total information technology budget on security. Another 23% spend over 5%.[5]

Some portions of the private sector are required by law to take responsibility for protecting the information on their computer systems, primarily to protect certain personal information contained on those systems. The Gramm-Leach-Bliley Act (Title V of P.L. 106-102) requires certain financial firms to protect the financial information of their clients, and the Health Insurance Portability and Accountability Act of 1996 (Title II, Subtitle F of P.L. 104-191) requires certain health care delivery firms to protect personal health-related information. To the extent that much of this information resides on private sector computer systems, the federal government is indirectly involving itself in the security of a subset of private computer systems. More recently, a provision in the Sarbannes-Oxley Act of 2002 (P.L. 107-204, Sec.404) requires certain corporations to certify the integrity of their financial control systems as part of their annual reporting requirements. Again, to the extent that a corporation's financial information and controls exist on computer systems, the federal government has extended indirectly its involvement in the security of private sector computer systems. It is not clear how these efforts have affected the overall security of the Internet.

Most experts agree that much more can be done to make the Internet and its users more secure. Aside from the inherent vulnerabilities associated with highly interconnected information networks, two major sources of vulnerabilities exist: software and network configurations/management. Operating systems and applications developers say they are paying greater attention to designing better security into their software products. But it is still 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.[6] Many intrusions take advantage of software vulnerabilities noted many months earlier, for which fixes have already been offered. Also, the pace at which new products, services, and hardware become available makes managing system changes and complexity increasingly difficult.

---

[4] The link to this article is no longer available.

[5] CSI/FBI Survey, 2004. p.5.

[6] The *National Strategy to Secure Cyberspace* recommends ways to make it easier for users to update the latest security-related patches.

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. 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.[7] 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. Some in the security community feel that security will not improve without some requirements imposed upon the private sector. However, both users and vendors of computer software suggest that the market is sufficient to address security in the most cost-effective manner. The Bush Administration, as the Clinton Administration before it, has chosen to use engagement and not regulation to encourage the private sector to improve security. However, both Administrations did not rule out the use of regulation if necessary.

Congress has shown, and continues to show, a strong interest in the security of computers and the Internet. This interest to date, however, has largely been manifested in numerous oversight hearings by a multitude of committees and subcommittees, in both the House and the Senate. Legislatively, Congress has been more circumspect. The 108th Congress did not pass any major legislation related to improving the security of the Internet. Many bills were introduced that touched upon, either directly or indirectly, Internet or computer security. For example, S. 187 (Edwards) would have required federal Chief Information Officers (CIOs) to identify their agency's network vulnerabilities, set performance goals for addressing those vulnerabilities, and evaluate how those performance goals are being met on a quarterly basis. It also would have instructed the National Institute of Standards and Technology to develop guidelines to assist CIOs in this task. S. 1633 (Corzine) and H.R. 3233 (Gutierrez) would have required financial firms to notify customers of unauthorized use of personal information maintained by those firms. H.R. 1636 (Stearns) would have required companies to effect adequate information security policies to protect personal information of customers and to take remedial action to information security advisories issues by the Department of Homeland Security. H.R. 3159 (Waxman) would have specifically included in the federal information security requirements protections of information shared via peer-to-peer programs. S. 779 (Jeffords) and S. 1039 (Inhofe) would have required wastewater facilities to conduct vulnerability studies that would include assessing vulnerabilities of facility information. H.R. 3562 (Shuster) would have offered tax credits to cover part of the cost of deploying building security devices. The list of qualifying devices included computers and software used to combat cyberterrorism. H.R. 5068 (Thornberry) would have elevated cybersecurity within the Department of Homeland Security by establishing the position of Assistant Secretary for Cybersecurity within the Information Analysis and Infrastructure Protection Directorate.

---

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

For an overview of federal legislation, executive orders, and presidential directives associated with computer and Internet security, see CRS Report RL32357, *Computer Security: A Summary of Selected Federal Laws, Executive Orders, and Presidential Directives*.

Broadband Internet Access[8]

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."

On March 26, 2004, President Bush endorsed the goal of universal broadband access by 2007.[9] Then on April 26, citing that the U.S. ranks 10th in the world in broadband deployment, President Bush announced a broadband initiative which advocates permanently prohibiting all broadband taxes, making spectrum available for wireless broadband, creating technical standards for broadband over power lines, and simplifying rights-of-way processes on federal lands for broadband providers.[10]

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. Congress continues to debate proposed approaches to addressing broadband deployment, including easing restrictions and requirements on incumbent telephone companies and providing federal financial assistance for broadband deployment in rural and economically disadvantaged areas.

---

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

[9] Allen, Mike, "Bush Sets Internet Access Goal," *Washington Post*, March 27, 2004.

[10] See White House, *A New Generation of American Innovation*, April 2004. Available at [http://www.whitehouse.gov/infocus/technology/economic_policy200404/innovation.pdf]

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) 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. Whether such requirements are necessary to ensure the development of competition and its subsequent consumer benefits, or are overly burdensome and only discourage needed investment in and deployment of broadband services has been the focus of the policy debate.

Unbundling and Resale. Present law requires all ILECs to open up their networks to enable competitors to lease out parts of the incumbent's network. These unbundling and resale requirements, which are detailed in Section 251 of the Telecommunications Act of 1996, were enacted in an attempt to open up the local telephone network to competitors. Under these provisions, ILECs are required to grant competitors access to individual pieces, or elements, of their networks (e.g., a line or a switch) and to sell them at below retail prices.

The FCC, in a February 2003 split decision, modified the regulatory framework regarding how ILECs and competitors interact in the telecommunications marketplace. The "triennial review"order (TRO) (CC Docket 01-338), which was released in August 2003, established new guidelines regarding how ILECs must make their networks available to competitors. Included in the FCC's decision were provisions which: no longer required, over a transition period, that line sharing be an unbundled network element and during each year of the transition increased incrementally the price for the high frequency portion of the loop; eliminated unbundling for switching for business customers using high capacity loops, but gave state utility commissions 90 days to rebut the national finding; gives state commissions nine months to make geographic specific determinations regarding the availability of unbundled elements and the unbundled network element platform (UNE-P); removed unbundling requirements on newly deployed hybrid (fiber-copper) loops but ensured continued access to existing copper and removes unbundling requirements on all newly deployed fiber to the home. (A summary of this order can be found at *Federal Register* Vol. 68, No. 169, September 2, 2003, p. 52276.)

Court challenges to this order were consolidated (USTA v. FCC) in the U.S. Court of Appeals, D.C. Circuit. In a March 2, 2004 decision, the court vacated a number of key provisions of the TRO, including those dealing with unbundling and delegation of state authority. Claiming that the FCC's conclusions were based on broad assumptions and "...do not support a non-provisional national impairment finding" and that the FCC's definition of impairment "is vague almost to the point of being empty," the Court vacated provisions that call for the unbundling of mass

market switching. Similarly, the Court also vacated the FCC's nationwide impairment findings for dedicated transport (e.g. DS-1, DS-3 and dark fiber). Provisions in the TRO that delegate to the states the authority to make determinations regarding the presence of market impairment were also deemed unlawful. According to the court, Congress in the 1996 Act did not "... delegate to the FCC the authority to subdelegate to outside parties [the states]." The Court ruled that it was unlawful for the FCC to give to the states the authority to have such a major role in determining the range of network elements the CLECs should have access to and the use of the UNE-P. (However, the Court did uphold the authority given to the states to petition the FCC to waive, for specific markets, the general "no impairment" finding reached by the FCC over unbundled switching for the enterprise [large business] market.)

The Court, however, upheld the broadband provisions of the order including those that phase out line sharing and remove unbundling requirements for newly deployed hybrid loops and fiber- to-the-home. While the Court did concede that some impairment might exist, it found that "... the Commission [FCC] reasonably found that other considerations [e.g., the encouragement of facilities based competition, the need to give incumbents greater incentives to invest in their own infrastructure, and the overall policy goal of Section 706 of the 1996 Telecommunications Act to ensure the nationwide deployment of advanced services] outweighed any impairment." While the Court ordered a 60-day stay (until May 3, 2004) of the ruling pending appeal, the FCC requested and was granted a 45-day extension (until June 15, 2004) during which negotiation of commercial agreements on network access were undertaken. To date, a few commercial agreements have been announced. A decision by the Solicitor General and the FCC not to appeal the ruling to the U.S. Supreme Court and a subsequent refusal by the Supreme Court to stay the Appeals Court ruling have resulted in the implementation of the ruling as of June 15, 2004. The focus has now shifted to three forums: to the FCC as it attempts to establish permanent rules consistent with the Appeals Court ruling (See *Federal Register*, Vol. 69, No. 176, September 13, 2004, p. 55128); to the industry players as they continue to negotiate access agreements; and to the D.C. U.S. Appeals Court where a petition seeking to vacate the FCC established interim rules and require implementation of the court's March 2004 decision is being held by the court until January 4, 2005.

Provision of InterLATA Services. As a result of the 1984 AT&T divestiture, the Bell System service territory was broken up into service regions and assigned to regional Bell operating companies (BOCs). The geographic area in which a BOC may provide telephone services within its region was further divided into local access and transport areas, or LATAs. These LATAs total 164 and vary dramatically in size. LATAs generally contain one major metropolitan area and a BOC will have numerous LATAs within its designated service region.

Telephone traffic that crosses LATA boundaries is referred to as interLATA traffic. Restrictions contained in Section 271 of the Telecommunications Act of 1996 prohibit the BOCs from offering interLATA services within their service regions until certain conditions are met. BOCs seeking to provide such services must file an application with the FCC and the appropriate state regulatory authority that demonstrates compliance with a 14-point competitive checklist of market-opening requirements. The FCC, after consultation with the Justice Department and the

relevant state regulatory commission, determines whether the BOC is in compliance and can be authorized to provide in-region interLATA services.

As of December 3, 2003, all four BOCs — Verizon, SBC Communications, BellSouth and West — had received approval to enter the in-region interLATA market. Now that the approval process has been completed, the FCC's role shifts to monitoring to ensure compliance. Under the terms and conditions of the 1996 Act, the FCC is required to monitor the BOCs to ensure compliance with the terms agreed to when they were granted long distance approval. If the FCC determines that a BOC is not fulfilling those terms, the FCC is required to order corrections, impose penalties, or suspend or revoke approval. The independent telephone companies, or non-BOC providers of local service, are not subject to these restrictions and were not required to file for approval to carry telephone traffic regardless of whether it crosses LATA boundaries.[11]

Federal Assistance for Broadband Deployment

In the 108th Congress, legislation was introduced to provide financial assistance to encourage broadband deployment, and to allocate additional spectrum for use by wireless broadband applications. The FY2005 Consolidated Appropriations Act (P.L. 108-447) provides continued funding in FY2005 for the Rural Broadband Access Loan and Loan Guarantee Program and the Community Connect Broadband Grants in the Rural Utilities Service (RUS) of the U.S. Department of Agriculture. Also passed in the 108th Congress was the Commercial Spectrum Enhancement Act (Title II of H.R. 5419, P.L. 108-494), which seeks to make more spectrum available for wireless broadband and other services by facilitating the reallocation of spectrum from government to commercial users. For more information on federal assistance for broadband deployment, see CRS Report RL30719, *Broadband and the Digital Divide: Federal Assistance Programs*.

Electronic Commerce[12]

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."

---

[11] For a more complete discussion of LATAs and BOC long distance entry see CRS Report RL30018, *Long Distance Telephony: Bell Operating Company Entry Into the Long-Distance Market*, by James R. Riehl.

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

Since the late 1990s, commercial transactions on the Internet have grown substantially.[13] 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 "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. 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 Asia 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. 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. 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 the end of 2003, that sector of the U.S. economy will reach

---

[13] For statistics and other data on e-commerce, see CRS Report RL31270, *Internet Statistics: Explanation and Sources*. 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.

$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.

Issues for the Bush Administration and Congress

Concurrent with the growth of commercial electronic transactions, 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 the September 11, 2001 terrorist attacks. The 108th Congress passed a bill, signed into law (P.L. 108-435) by President Bush, that for the second time extended the moratorium on domestic e-commerce taxation to November 2007. In addition, congressional policymakers are looking at the European Union (EU) and World Trade Organization (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.

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 imposed a three-year moratorium on the ability of state and local governments to levy certain taxes on the Internet; it prohibited taxes on Internet access, unless such a tax was generally imposed and actually enforced prior to October 1, 1998; it created 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 opposed 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 (Cox), the Internet Tax Nondiscrimination Act, extended the Internet tax moratorium through November 1, 2003 (P.L. 107-75). The 108th Congress, facing the expiration of the moratorium, passed S. 150, the Internet Tax Non-Discrimination Act of 2003 (Allen). Among its provisions, the bill: 1) extended the e-commerce tax moratorium for four years, from November 1, 2003 through November 1, 2007; 2) expanded the definition of Internet access to include both providers and buyers of Internet access; 3) grandfathered through November 1, 2007, Internet access taxes enforced before October 1, 1998; 4) similarly grandfathered through November 1, 2005 Internet access taxes enforced before November 1, 2003; and 5) excluded Voice Over Internet Protocol (VoIP) and similar voice services. President Bush signed S. 150 into law on December 3, 2004 (P.L. 108-435). See also: CRS Report RL31929, *Internet Taxation: Issues and Legislation of the 108th Congress*, 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. Among the issues considered by the WTO has been 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. The WTO also has developed a work program on electronic commerce and to report on the progress of the work program, with recommendations, as well as continuing the practice of not imposing tariffs on electronic transmissions. Future WTO meetings 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).*

"Spam": Unsolicited Commercial Electronic Mail[14]

One aspect of increased use of the Internet for electronic mail (e-mail) has been the advent of unsolicited advertising, also called "unsolicited commercial e-mail (UCE)," "unsolicited bulk e-mail," "junk e-mail, "or "spam." Complaints focus on the fact that some spam contains or has links to pornography, that much of it is fraudulent, that it is a nuisance, and the volume of spam is increasing.

In 2003, Congress passed a federal anti-spam law, the CAN-SPAM Act (P.L. 108-187), which became effective on January 1, 2004. The act preempts state laws that specifically address spam but not state laws that are not specific to e-mail, such as trespass, contract, or tort law, or other state laws to the extent they relate to fraud or computer crime. It does not ban unsolicited commercial e-mail. Rather, it allows marketers to send commercial e-mail as long as it conforms with the law, such as including a legitimate opportunity for consumers to "opt-out" of receiving future commercial e-mails from that sender. It does not require a centralized "do not e-mail" registry to be created by the Federal Trade Commission (FTC), similar to the National Do Not Call registry for telemarketing. The bill requires only that the FTC develop a plan and timetable for establishing a "do not e-mail" registry and to inform Congress of any concerns it has with regard to establishing it. The FTC reported to Congress in June 2004 that without a technical system to authenticate the origin of e-mail messages, a Do Not Email registry would not reduce the amount of spam, and, in fact, might increase it. Authentication is a technical approach that could be used to control spam that is under study by a number of groups, including ISPs, who are attempting to develop a single authentication standard for the industry. The Anti-Spam Technical Alliance, which includes Microsoft, AOL, Yahoo!, and Earthlink, announced in July 2004 that they had chosen a standard, called Sender ID, but it was rejected by an industry-wide advisory group because of intellectual property issues. Industry representatives are continuing to attempt to develop a standard.

Many argue that technical approaches, such as authentication and consumer education, are needed to solve the spam problem — that legislation alone is insufficient. Nonetheless, there is considerable interest in assessing how effective the CAN-SPAM Act is in reducing spam. The effectiveness of the law may be difficult to determine, however, if for no other reason than there are various definitions of spam. Proponents of the law argue that consumers are most irritated by *fraudulent* e-mail, and that the law should reduce the volume of such e-mail because of the civil and criminal penalties included therein. Opponents counter that

---

[14] See also CRS Report RL31953, *"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.

consumers object to *unsolicited* commercial e-mail, and since the bill legitimizes commercial e-mail (as long as it conforms with the law's provisions), consumers actually may receive more, not fewer, unsolicited commercial e-mail messages. Thus, whether "spam" is reduced depends in part on whether it is defined as only fraudulent commercial e-mail or as all unsolicited commercial e-mail. A survey of 2,000 e-mail users released by Consumers Union (CU) in August 2004 found that spam comprised more than half of the e-mail of 69% of the respondents, and, three months after the law went into effect, 47% said that they were receiving more spam, not less.[15]

Some critics of the law want legislation that would require consumers to give their express consent — to "opt-in" — before marketers could send e-mails. California passed such a law, which was to become effective January 1, 2004, but the CAN-SPAM Act preempted it. The European Union adopted an opt-in approach for unsolicited commercial e-mail, unless there is an existing customer relationship, that went into effect on October 31, 2003. (Individual EU countries must pass their own legislation to implement the EU directive; not all have done so yet.) The CAN-SPAM Act is discussed in more detail in CRS Report RL31953.

Although consumers are most familiar with spam on their personal computers, it also is becoming an issue in text messaging on wireless telephones, pagers, and personal digital assistants (PDAs). The CAN-SPAM Act included a provision requiring the Federal Communications Commission (FCC) to establish regulations to protect wireless consumers from spam. The FCC issued those rules in August 2004. See CRS Report RL31636 for more on wireless privacy and wireless spam.

Internet Domain Names[16]

The 108th Congress continued 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.

---

[15] Consumers Union. Consumer Reports Investigates How to Protect Against Spam, Spyware and Phishing. Press Release, August 9, 20004. [http://www.consumersunion.org/pub/core_product_safety/001305.html#more]

[16] 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.

Background

The Internet originated with research funding provided by the Department of Defense Advanced Research Projects Agency (DARPA) to establish a military 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 five-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 provided that VeriSign would 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.

On September 17, 2003, ICANN and the Department of Commerce agreed to extend their MOU until September 30, 2006. The MOU specifies transition tasks which ICANN has agreed to address. ICANN will implement an objective process for selecting new Top Level Domains; implement an effective strategy for multi-lingual communications and international outreach; and develop a contingency plan, consistent with the international nature of the Internet, to ensure continuity of operations in the event of a severe disruption of operations.

Issues

The Department of Commerce remains responsible for monitoring the extent to which ICANN satisfies the principles of the White Paper as it makes critical DNS decisions. Congress remains interested in how the Administration manages and oversees the transition to private sector ownership of the DNS.

Top Level Domains. 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. Subsequently, ICANN considered eleven applications for operating .org after the agreement with VeriSign expired on December 31, 2002. On October 14, 2002, the ICANN Board selected the Internet Society's Public Interest Registry as .org operator. On December 15, 2003, ICANN formally invited applications from all parties for new TLDs. The application period closed on March 15, 2004; ten applications were received. ICANN has entered into negotiations on approving four of the candidate TLDs. Meanwhile, in December 2004, ICANN issued a request for proposals for operating the .net registry.

Protecting Children on the Internet. In the 107th Congress, legislation sought to create a "kids-friendly top level domain name" that would contain only age-appropriate content. The Dot Kids Implementation and Efficiency Act of 2002 was signed into law on December 4, 2002 (P.L. 107-317) and authorizes the National Telecommunications and Information Administration (NTIA) to require the .us registry operator (currently NeuStar) to establish, operate, and maintain a second level domain within the .us TLD that is restricted to material suitable for minors. (For more information on the Dot Kids Act, and other legislative attempts to protect children from unsuitable material on the Internet, see CRS Report RS21328).

The 108th Congress passed the PROTECT Act (P.L. 108-21), which contains a provision (Sec. 108: Misleading Domain Names on the Internet) which would make

it a punishable crime to knowingly use a misleading domain name with the intent to deceive a person into viewing obscenity on the Internet. Increased penalties are provided for deceiving minors into viewing harmful material.

Governance. 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. New bylaws based on the reform proposal were formally adopted by the ICANN Board at the October 2002 Board meeting in Shanghai. Some in the Internet community have spoken against the ICANN reforms, asserting that its elimination of elected At-Large board members precludes effective representation of unaffiliated Internet users. In a related development, the United Nations, at the December 2003 World Summit on the Information Society (WSIS), debated and agreed to study the issue of whether national governments should run the domain name system instead of ICANN. The study is being conducted by the UN's Working Group on Internet Governance (WGIG). The United Nations will revisit the issue in 2005, after the WGIG study is complete. On December 22, 2004, ICANN announced that it will contribute $100,000 to help support the WGIG study.

Trademark Disputes. 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.

Meanwhile, the 106th Congress passed 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, and provides for statutory civil damages of at least $1,000, but not more than $100,000, per domain name identifier.

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. WIPO did not recommend new rules regarding personal, geographical, or trade names.

In the 108th Congress, H.R. 3754 (Fraudulent Online Identities Sanctions Act) was reported by the Committee on the Judiciary on June 9, 2004 (H.Rept. 108-536). H.R. 3754 would increase criminal penalties for those who submit false contact information (maintained in the "whois" database) when registering a domain name that is subsequently used to commit a crime or engage in copyright or trademark infringement. The legislation was subsequently enacted as Title II of H.R. 3632, the Intellectual Property Protection and Courts Amendments Act of 2004 (P.L. 108-482).

Government Information Technology Management[17]

The evolving role of the Internet in the political economy of the United States continues to attract increased congressional attention to government information technology management issues. Interest has been further heightened by national information infrastructure development efforts, e-government projects, and homeland security initiatives. Although wide-ranging, most government information technology management issues focus on information technology research and development, the provision of online services by the government ("e-government"), and availability and use of "open source" software.

Internet Infrastructure: NTIA's Role

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. For FY2005, Congress has eliminated funding for the Technology Opportunity Program (TOP), which has provided matching merit-based grants to areas either underserved or not served at all by the Internet. Still, some policymakers support a stronger role for NTIA to close the divide between the nation's Internet"haves" and "have-nots." They contend that NTIA's funding of TOP grants would be an appropriate avenue for helping bridge this divide.

Information Technology R&D[18]

At the federal level, almost all of the funding for information science and technology and Internet development is part of a single government-wide initiative, the Networking and Information Technology Research and Development program (NITRD). This program was previously (1997-2000) called the Computing, Information, and Communications program (CIC) and, prior to that (1992-1997), the

---

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

[18] See also CRS Issue Brief IB10130, *The Federal Networking and Information Technology Research and Development Program; Funding Issues and Activities*, by Patricia Moloney Figliola.

High Performance Computing and Communications program (HPCC). The NITRD is an interagency effort to coordinate key advances in information technology (IT) research and leverage funding into broader advances in computing and networking technologies. Under the NITRD, participating agencies receive support for high-performance computing science and technology, information technology software and hardware, networks and Internet-driven applications, and education and training for personnel.

For FY2005, the President requested a budget of $2.0 billion for NITRD activities. The final amount appropriated has not yet been determined, as appropriations across the NITRD agencies must be calculated. However, the final budget is usually in line with the President's request. (See CRS Issue Brief IB10130 for updated information.) The majority of funding goes to the National Science Foundation, National Institutes of Health, National Aeronautics and Space Administration, Defense Advanced Research Projects Agency, and the Department of Energy's Office of Science.

Research emphases are focused on six program component areas (also called PCAs): high-end computing research; human computer interaction and information management; large-scale networking; software design and productivity; high-confidence software and systems; and social, economic, and workforce implications of IT and IT workforce development. Key issues facing congressional policymakers include the following: is NITRD accomplishing its goals and objectives to enhance U.S. information technology research and development; is the funding level appropriate or should it be changed to reflect changing U.S. priorities; and what should be the private sector's role in this federal initiative?

Electronic Government (E-Government)[19]

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 area of concern is developing a comprehensive but flexible strategy to coordinate the disparate e-government initiatives across the federal government.

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

---

[19] CRS Report RL31057, *A Primer on E-Government: Sectors, Stages, Opportunities, and Challenges of Online Governance*, by Jeffrey W. Seifert, which is updated more frequently than this report.

(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 now-discontinued eBillPay service, which allowed consumers to schedule and make payments to creditors online [http://www.usps.com/paymentservices/ops_discontinued.htm].

E-government initiatives vary significantly in their breadth and depth from state to state and agency to agency. Perhaps one of the most well-known federal examples is the FirstGov website [http://www.firstgov.gov]. FirstGov 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 Grants.gov initiative [http://www.grants.gov/], which is designed to provide a single portal for all available federal grants, enabling users to search, download applications, and apply for grants online. At the Department of Treasury, the Internal Revenue Service (IRS) administers the Free File initiative [http://www.irs.gov/efile/article/0,,id=118986,00.html], which has partnered with industry to provide free online tax preparation and electronic filing services for eligible taxpayers.

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.[20] In doing so, the Task Force identified 23 interagency initiatives designed to better integrate agency operations and information technology investments. These initiatives, sometimes referred to as the Quicksilver projects, 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 by the President's Management Council. In 2002 the e-Clearance initiative, originally included as part of the Enterprise Human Resources Integration project, was established as a separate project, for a total of 25 initiatives. As the initial round of e-government projects continue to develop, OMB has stated it plans to focus attention on initiatives that consolidate information technology systems in six functional areas, or lines of business. These include data and statistics, human resources, criminal investigations, financial management, public health monitoring, and monetary benefits.

---

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

On December 17, 2002, President Bush signed the E-Government Act of 2002 (P.L. 107-347) into law. The law contains a variety of provisions related to federal government information technology management, information security, and the provision of services and information electronically. One of the most recognized provisions involves the creation of an Office of Electronic Government within OMB. The Office is headed by an Administrator, who is responsible for carrying out a variety of information resources management (IRM) functions, as well as administering the interagency E-Government Fund provided for by the law.

For the 109th Congress, oversight of the Quicksilver projects, the implementation of the E-Government Act, and the development of a second group of e-government projects are anticipated to be significant issues. Other related issues include ongoing efforts to develop a federal enterprise architecture, which serves as a blueprint of the business functions of an organization, and the technology used to carry out these functions [http://www.feapmo.gov/]; the recruitment and retention of IT managers, at both the chief information officer (CIO) and project manager levels; and balancing the sometimes competing demands of e-government and homeland security.

Open Source Software[21]

The use of open source software by the federal government has been gaining attention as organizations continue to search for opportunities to enhance their information technology (IT) operations while containing costs. For the federal government and Congress, the debate over the use of open source software intersects several other issues, including, but not limited to, the development of homeland security and e-government initiatives, improving government information technology management practices, strengthening computer security, and protecting intellectual property rights. In the 109th Congress, the debate over open source software is anticipated to revolve primarily around information security and intellectual property rights. However, issues related to cost and quality are likely to be raised as well.

Open source software refers to a computer program whose source code, or programming instructions, is made available to the general public to be improved or modified as the user wishes. Some examples of open source software include the Linux operating system and Apache Web server software. In contrast, *closed source*, or proprietary, programs are those whose source code is not made available and can only be altered by the software manufacturer. In the case of closed source software, updates to a program are usually distributed in the form of a patch or as a new version of the program that the user can install but not alter. Some examples of closed source software include Microsoft Word and Corel WordPerfect. The majority of software products most commonly used, such as operating systems, word processing programs, and databases, are closed source programs.

---

[21] See also CRS Report RL31627, *Computer Software and Open Source Issues: A Primer*, by Jeffrey W. Seifert, which is updated more frequently than this report.

For proponents, open source software is often viewed as a means to reduce an organization's dependence on the software products of a few companies while possibly improving the security and stability of one's computing infrastructure. For critics, open source software is often viewed as a threat to intellectual property rights with unproven cost and quality benefits. So far there appear to be no systematic analyses available that have conclusively compared closed source to open source software on the issue of security. In practice, computer security is highly dependent on how an application is configured, maintained, and monitored. Similarly, the costs of implementing an open source solution are dependent upon factors such as the cost of acquiring the hardware/software, investments in training for IT personnel and end users, maintenance and support costs, and the resources required to convert data and applications to work in the new computing environment. Consequently, some computer experts suggest that it is not possible to conclude that either open source or closed source software is inherently more secure or more cost efficient.

The growing emphasis on improved information security and critical infrastructure protection overall, will likely be an influential factor in future decisions to implement open source solutions. The rapidly changing computer environment may also foster the use of a combination of open source and closed source applications, rather than creating a need to choose one option at the exclusion of another.

Appendix A: 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
DSL	Digital Subscriber Line
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	generic 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
OSS	Open Source Software
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
DSL	Digital Subscriber Line
gTLD	generic Top Level Domain
IP	Internet Protocol
IT	Information Technology
LATA	Local Access and Transport Area
NGI	Next Generation Internet
OSS	Open Source Software
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 B: Legislation Passed by the 105th - 107th 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 website 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 website, 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 websites.

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 websites 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

Legislation Enacted in the 107th Congress

Internet Privacy

The 107th Congress passed four laws affecting Internet privacy. The **USA PATRIOT Act (P.L. 107-56)**, passed in the wake of the September 11, 2001 terrorist attacks, *inter alia* expands law enforcement's authority to monitor Internet activities. The Cyber Security Enhancement Act, included as section 225 of the Homeland Security Act (P.L. 107-296), amends the USA PATRIOT Act to further loosen restrictions on Internet Service Providers (ISPs) as to when, and to whom, they can voluntarily release information about subscribers.

Prior to the terrorist attacks, concern had focused on the opposite issue — whether law enforcement officials might be overstepping their authority when using a software program named Carnivore (later renamed DCS 1000) to monitor Internet activities. Although the USA PATRIOT Act expands law enforcement's authority to monitor Internet activities, Congress also passed a provision in the **21st Century Department of Justice Authorization Act (P.L. 107-273, section 305)** requiring the Justice Department to notify Congress about its use of Carnivore or similar systems.

Congress also passed the **E-Government Act (P.L. 107-347)** that, *inter alia*, sets requirements on government agencies in how they assure the privacy of personal information in government information systems and establish guidelines for privacy policies for federal websites.

Broadband Internet Access

The **Farm Security and Rural Investment Act of 2002 (P.L. 107-171, Section 6103)** authorizes the Secretary of Agriculture to make loans and loan guarantees to eligible entities for facilities and equipment providing broadband service in rural communities. The **National Science Foundation Authorization Act of 2002 (P.L. 107-368, Section 18(d))** directs the National Science Foundation to conduct a study of broadband network access for schools and libraries.

Electronic Commerce

The **Internet Tax Nondiscrimination Act (P.L. 107-75)** extends the Internet tax moratorium through November 1, 2003.

Internet Domain Names

The **Dot Kids Implementation and Efficiency Act of 2002 (P.L. 107-317)** directs the National Telecommunications and Information Administration of the Department of Commerce to require the .us registry operator to establish, operate, and maintain a second level domain that is restricted to material suitable for minors.

E-Government

The **E-Government Act of 2002** amends Title 44 U.S.C. by adding Chapter 36 — Management and Promotion of Electronic Government Services, and Chapter 37 — Information Technology Management Program, which includes a variety of provisions related to information technology management and the provision of e-government services. Among its provisions, the law establishes an Office of Electronic Government in the Office of Management and Budget to be headed by an Administrator appointed by the President. It also authorizes $345 million through FY2006 for an E-Government Fund to support initiatives, including interagency and intergovernmental projects, that involve the "development and implementation of innovative uses of the Internet or other electronic methods, to conduct activities electronically." Additionally, the law includes language that re-authorizes and amends the Government Information Security Reform Act (GISRA), establishes an information technology worker exchange program between the federal government and the private sector, promotes the use of Share-In-Savings procurement contracts, and establishes coordination and oversight policies for the protection of confidential information and statistical efficiency (the Confidential Information Protection and Statistical Efficiency Act of 2002).

Summary of Legislation Passed by 107th Congress

Title	Public Law Number
Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism (USA PATRIOT) Act	P.L. 107-56
Internet Tax Nondiscrimination Act	P.L. 107-75
Farm Security and Rural Investment Act (Section 6103)	P.L. 107-171
Cyber Security Enhancement Act (Section 225 of the Homeland Security Act)	P.L. 107-296
21st Century Department of Justice Authorization Act (Section 305)	P.L. 107-297
Dot Kids Implementation and Efficiency Act	P.L. 107-317
E-Government Act	P.L. 107-347
National Science Foundation Authorization Act of 2002 (Section 18d)	P.L. 107-368

Appendix C: Related CRS Reports

Internet Privacy

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

CRS Report RS21906. *9/11 Commission Recommendations: A Civil Liberties Oversight Board*, 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 RS21851. *Privacy Protection: Mandating New Arrangements to Implement and Assess Federal Privacy Policy and Practices*, by Harold C. Relyea.

CRS Report RL32706. *Spyware: Background and Policy Issues for Congress*, by Marcia S. Smith.

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.

CRS Report RS21704. *USA PATRIOT Act Sunset: A Sketch*, by Charles Doyle.

CRS Report RL32186. *USA PATRIOT Act Sunset: Provisions that Expire on December 31, 2005*, by Charles Doyle.

Computer Security

CRS Report RL32357. *Computer Security: A Summary of Selected Federal Laws, Executive Orders, and Presidential Directives*, by John Moteff.

CRS Report RL30153. *Critical Infrastructures: Background, Policy, and Implementation*, by John D. Moteff.

CRS Report RL32331. *The Economic Impact of Cyber-Attacks*, by Brian Cashell, William D. Jackson, Mark Jickling, and Baird Webel.

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 RL31542. *Homeland Security — Reducing the Vulnerability of Public and Private Information Infrastructures from Terrorism: An Overview*, by Jeffrey Seifert.

CRS Report RL31787. *Information Warfare and Cyberwar: Capabilities and Related Policy Issues*, by Clay Wilson.

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 RL32421. *Broadband over Powerlines: Regulatory and Policy Issues*, by Patricia Moloney Figliola.

CRS Report RL31938. *Local Telephone Competition: A Brief Overview*, by Angele A. Gilroy.

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.

CRS Report RS20993. *Wireless Technology and Spectrum Demand: Third Generation (3G) and Beyond*, by Linda K. Moore.

Electronic Commerce

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

CRS Report RS21596. *EU Tax on Digitally Delivered E-Commerce*, by Martin A. Weiss and Nonna A. Noto.

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

CRS Report RL31929. *Internet Taxation: Issues and Legislation in the 108th Congress*, by Steven Maguire and Nonna A. Noto.

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 RS21537. *State Sales Taxation of Internet Transactions*, by John Luckey.

"Spam"

CRS Report RL31953. *"Spam": An Overview of Issues Concerning Commercial Electronic Mail*, by Marcia S. Smith.

CRS Report RL31488. *Regulation of Unsolicited Commercial E-Mail*, by Angie A. Welborn.

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 RL31627. *Computer Software and Open Source Issues: A Primer*, by Jeffrey W. Seifert.

CRS Report RL31594. *Congressional Continuity of Operations (COOP): An Overview of Concepts and Challenges*, by R. Eric Petersen and Jeffrey W. Seifert. 16 p.

CRS Report RL31857. *Continuity of Operations (COOP) in the Executive Branch: Background and Issues for Congress*, by R. Eric Petersen.

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

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

CRS Issue Brief IB10130. *The Federal Networking and Information Technology Research and Development Program: Funding Issues and Activities*, by Patricia Moloney Figliola.

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.

CRS Report RL32597. *Information Sharing for Homeland Security: An Overview*,by Harold C. Relyea and Jeffrey W. Seifert.

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

Copyright and "Fair Use"

CRS Report RL31626. *Copyright Law: Statutory Royalty Rates for Webcasters*, by Robin Jeweler.

CRS Report RL31827, *"Digital Rights" and Fair Use in Copyright Law*, by Robin Jeweler.

CRS Report RL32035. *Digital Rights Management Legislation*, by Robin Jeweler.

CRS Report RS21206. *"Fair Use" on the Internet: Copyright's Reproduction and Public Display Rights,* by Robin Jeweler.

Identity Theft

CRS Report RL32121. *Fair Credit Reporting Act: A Side-By-Side Comparison of House, Senate, and Conference Versions*, by Angie A. Welborn.

CRS Report RL31919. *Remedies Available to Victims of Identity Theft*, by Angie A. Wellborn.

Internet-General

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

Medical Records, Financial, and Other Privacy Issues

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

CRS Report RL30677. *Digital Surveillance: The Communications Assistance for Law Enforcement Act*, by Patricia Moloney Figliola.

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.

CRS Report RL31636. *Wireless Privacy and Spam: Issues for Congress*, by Marcia S. Smith.

Protecting Children

CRS Report RS21328. *Internet: Status of Legislative Attempts to Protect Children from Unsuitable Material on the Web*, by Marcia S. Smith and Amanda Jacobs.

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

Other Related Topics

CRS Report RL32232. *Bundling Residential Telephone, Internet, and Video Services: Issues for Congress*, by Charles B. Goldfarb.

CRS Report RS21647. *Facsimile Advertising Rules Under the Telephone Consumer Protection Act of 1991: Background and Status*, by Patricia Moloney Figliola.

CRS Report RL31642. *Regulation of the Telemarketing Industry: State and National Do-Not-Call Registries*, by Angie A. Welborn.

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

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