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 April 13, 2005

Marcia S. Smith, John D. Moteff, Lennard G. Kruger,
Jeffrey W. Seifert, and Patricia Moloney Figliola
Resources, Science, and Industry Division

Rita Tehan
Knowledge Services Group

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

Summary

In the decade between 1994 and 2004, the number of U.S. adults using the Internet increased from 15% to 64%. From electronic mail to accessing information to online purchasing ("electronic commerce"), the Internet touches almost every aspect of modern life. The extent to which use of the Internet continues to grow, however, may be affected by a number of technology policy issues being debated in Congress

First is the availability of high-speed — or "broadband" — Internet access. Broadband Internet access gives users the ability to send and receive data at speeds far greater than Internet access over traditional telephone lines. With deployment of broadband technologies accelerating, Congress is seeking to ensure fair competition and timely broadband deployment to all sectors and geographical locations of American society.

Next are a range of issues that reflect challenges faced by those who do use the Internet, such as security, privacy (including spyware and identity theft), unsolicited commercial electronic mail ("spam"), and protecting children from unsuitable material (such as pornography). Computer security also involves broader concerns, such as the vulnerability of the nation's critical infrastructures to cyber attacks.

Other issues include the administration and governance of the Internet's domain name system (DNS), which is in 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.

The evolving role of the Internet in the political economy of the United States also continues to attract congressional attention. Among the issues are what changes may be needed at the Federal Communications Commission in the Internet age, federal support for information technology research and development, provision of online services by the government ("e-government"), and availability and use of "open source" software by the government.

A number of laws already have been passed on many of these issues. Congress is monitoring the effectiveness of these laws, and assessing what other legislation may be needed. Several bills are pending in the 109th Congress, particularly on broadband deployment and Internet privacy (including identity theft). This report identifies that legislation, but does not track the status of the bills. Other CRS reports referenced in this document do track legislation, and the reader should consult those reports, which are updated more frequently that this one, for current information. This report is updated quarterly.

Contents

Introduction 1

Background: Internet Usage and E-Commerce Statistics 1
- Internet Usage in the United States 2
  - Trends 2
  - Number of Users 2
  - Geographic Distribution 2
- International Internet Usage 3
- E-Commerce 3

Broadband Internet Access 4
- Easing Restrictions and Requirements on
  - Incumbent Telephone Companies 4
  - Unbundling and Resale 5
  - Open Access 6
- Federal Assistance for Broadband Deployment 7

Computer and Internet Security 7

Internet Privacy 11
- Collection of Data by Website Operators and Fair Information Practices . . 11
  - Commercial Websites 11
  - Federal Websites 12
- Spyware 12
- Identity Theft and "Phishing" 12
- Monitoring of E-Mail and Web Activity 13
  - By Government and Law Enforcement Officials 13
  - By Employers 14
  - By E-Mail Service Providers 14

"Spam": Unsolicited Commercial Electronic Mail 15

Protecting Children from Unsuitable Material 16

Internet Domain Names 17
- Background 17
- Issues 18
  - Top Level Domains 18
  - Governance 19
  - Trademark Disputes 19
  - Privacy 20

Government Information Technology Management 20
- The Federal Communications Commission 21
- Information Technology R&D 22
- Electronic Government (E-Government) 22
- Open Source Software 24

Appendix A: List of Pending Legislation 26
Broadband Internet Access 26
Internet Privacy 26
Government IT 27

Appendix B: List of Acronyms 28

Appendix C: Legislation Passed by the 105th - 108th Congresses 31

Appendix D: Related CRS Reports 39

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 technology policy issues being debated by Congress. Among them are access to broadband (high-speed) Internet services, computer and Internet security, Internet privacy, the impact of "spam," concerns about what children may encounter (such as pornography) when using the Internet, management of the Internet Domain Name System, and government information technology management.

This report provides overviews of those issues, plus appendices providing a list of related legislation pending before Congress, a list of acronyms, a discussion of related legislation passed in earlier Congresses, and a list of other CRS reports that provide more detail on these and related topics. Other issues that are not directly related to technology could also affect the use and growth of the Internet, such as intellectual property rights. Those issues are not addressed in this report, but the list of CRS products in Appendix D includes several that are on these related topics.

Because this report is updated only quarterly, it does not attempt to track legislation. For more timely information, see the other CRS reports identified in the following sections and in Appendix D.

Background: Internet Usage and E-Commerce Statistics[1]

According to the Pew Internet & American Life Project,[2] the percentage of adults (age 18 or older) in the United States using the Internet increased from approximately 15% in 1994, to 63% (or 128 million) in mid-2004. It also found that 81% of teenagers (age 12-17) use the Internet. On a typical day at the end of 2004, the Pew report shows, about 70 million American adults logged onto the Internet to use e-mail, read news, access government information, buy merchandise, and engage in countless other activities.

---

[1] By Rita Tehan, Knowledge Services Group.

[2] Pew Internet and American Life Project. Internet: the Mainstreaming of Online Life. January 25, 2005. See [http://www.pewinternet.org/pdfs/Internet_Status_2005.pdf]

Internet Usage in the United States

Trends. *Surveying the Digital Future, Year Four: Ten Years, Ten Trends*[3] highlights the major findings in Year Four of the Annenberg School's Digital Future Project, which is studying the impact of the Internet on Americans. Among the findings are:

- Internet access has risen to its highest level ever. About three-quarters of Americans now go online.
- The number of hours spent online continues to increase, rising to an average of 12.5 hours per week.
- Although the Internet has become the most important source of current information for users, the initially high level of credibility of information on the Internet began to drop in the third year of the study, and declined even further in Year Four.
- The number of users who believe that only about half of the information on the Internet is accurate and reliable is growing and has now passed 40 % of users for the first time.

Number of Users. The Federal Communications Commission (FCC) issues biannual reports on broadband Internet access service.[4] In its December 2004 report, the FCC reported that high-speed lines connecting homes and businesses to the Internet increased by 15% during the first half of 2004, from 28.2 million to 32.5 million lines. For the full twelve-month period ending June 30, 2004, high-speed lines increased by 38%.

Of the 32.5 million high-speed lines in service, 30.1 million served residential and small business subscribers, a 16% increase from the 26.0 million residential and small business high-speed lines reported six months earlier. For the 12-month period ending June 30, 2004, high-speed lines for residential and small business subscribers increased by 46%.[5]

Geographic Distribution. *A Nation Online: Entering the Broadband Age* is the sixth report released by the U.S. Department of Commerce examining Americans' use of computers, the Internet, and other information technology tools.[6]

---

[3] USC Annenberg School, Center for the Digital Future. The Digital Future Report: Surveying the Digital Future, Year Four: Ten Years, Ten Trends," September, 2004. See: [http://www.digitalcenter.org/downloads/DigitalFutureReport-Year4-2004.pdf]

[4] For the purposes of the FCC report, broadband means high-speed lines that deliver services exceeding 200 kilobits (kb) per second in at least one direction. Broadband Internet issues are discussed later in this report.

[5] FCC. Federal Communications Commission Releases Data on High-Speed Internet Access Services. Press release, December 22, 2004. Available at [http://www.fcc.gov/Bureaus/Common_Carrier/Reports/FCC-State_Link/IAD/hspd1204.pdf].

[6] U.S. Department of Commerce. A Nation Online: Entering the Broadband Age. September
(continued...)

The report also examines the geographic differences in broadband adoption and the reasons why some Americans do not have high-speed service. According to that September 2004 report, although the rate of Internet penetration among rural households (54.1%) was similar to that in urban areas (54.8%), the proportion of Internet users with home broadband connections remained much lower in rural areas than in urban areas.

International Internet Usage

According to a September 2004 report from the Computer Industry Almanac, the worldwide number of Internet users is expected to top 1 billion in 2005.[7] The report concluded that there is little Internet user growth in developed countries, but over the next five years, many Internet users in developing countries are expected to supplement computer-based Internet access with access via wireless devices. The Almanac also found that Internet use is growing strongly in China, and surpassed Japan for second place in 2003.

E-Commerce

The U.S. Census Bureau releases quarterly retail e-commerce statistics. On February 24, 2005, its estimate of U.S. retail e-commerce sales for the fourth quarter of 2004, adjusted for seasonal variation and holiday and trading-day differences, but not for price changes, was $18.4 billion, an increase of 4.7% from the third quarter of 2004. Total retail sales for the fourth quarter of 2004 were estimated at $938.5 billion.[8]

More than two thirds of online retail purchases are transacted via broadband, according to Nielsen//NetRatings MegaView Online Retail service, which tracks online consumer retail activity and purchasing behavior, and 69% of retail purchases transacted online were conducted via a broadband connection, compared to 31% transacted via narrowband or dial-up access during November 2004.[9]

---

[6] (...continued)
2004. See [http://www.ntia.doc.gov/reports/anol/index.html]. Rural/urban geographic distribution figures are on pp 15-19.

[7] Worldwide Internet Users will Top 1 Billion in 2005. Computer Industry Almanac, September 3, 2004. See [http://www.c-i-a.com/pr0904.htm]

[8] U.S. Census Bureau. Quarterly Retail E-commerce Sales, 4th Quarter 2004. See [http://www.census.gov/mrts/www/ecomm.html].

[9] Nielsen//NetRatings press release, January 19, 2005. See [http://www.nielsen-netratings.com/pr/pr_050119.pdf]

Broadband Internet Access[10]

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 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. 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.

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.

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. A related issue, whether and to what

---

[10] By Lennard G. Kruger, Resources, Science, and Industry Division. See also CRS Issue Brief IB10045, *Broadband Internet Access: Background and Issues*, which is updated more frequently than this report.

degree similar or competing services offered by different providers should be regulated, is also under review.

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.

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 FCC's implementation, with exceptions, of interim rules freezing current interconnection rates (i.e., those in place as of June 15,2004) and agreements for six months effective September 13, 2004, or until permanent rules are adopted, if earlier. The interim order also calls for a second subsequent six month phase, absent the adoption of permanent rules, that calls for some increase in ILEC rates for existing agreements but calls for the addition of new agreements at market-based rates.

In a December 15, 2004 action, the FCC adopted final unbundling rules in the TRO remand proceeding. In a 3-2 vote the FCC clarified the relationship between ILECs and competitor's access to the incumbents network elements. Included among these rules are those that eliminated, after a one-year phase out, unbundling for mass market (i.e., residential and small business market) local circuit switching (thereby eliminating the UNE-P); established a test to determine unbundling requirements for DS1 loops and transport; and dropped dark fiber loops from the list of elements the ILEC's must share with competitors. These rules took effect on March 11, 2005, replacing the interim rules released in August 2004.

The focus has now shifted to three forums: to the FCC as it attempts to implement the adopted, permanent rules; to the industry players as they continue to negotiate access agreements; and to the U.S. Court of Appeals, D.C. Circuit, where petitions challenging the FCC established rules have been consolidated for judicial review.

Open Access. Cities, counties, and states have taken up the issue of whether to mandate open access requirements on local cable franchises. In June 1999, a federal judge ruled that the city of Portland, Oregon had the right to require open access to the Tele-Communications Incorporated (TCI) broadband network as a condition for transferring its local cable television franchise to AT&T. AT&T appealed the ruling to the U.S. Court of Appeals for the Ninth Circuit. On June 22, 2000, the Court ruled in favor of AT&T, thereby reversing the earlier ruling. The court ruled that high-speed Internet access via a cable modem is defined as a "telecommunications service," and not subject to direct regulation by local franchising authorities. The debate then moved to the federal level, where many interpreted the Court's decision as giving the FCC authority to regulate broadband cable services as a "telecommunications service." On September 28, 2000, the FCC formally issued a Notice of Inquiry (NOI) to explore whether or not the Commission should require access to cable and other high-speed systems by Internet Service Providers (ISPs). On March 14, 2002, the FCC adopted a Declaratory Ruling which

classified cable modem service as an "interstate information service," subject to FCC jurisdiction and largely shielded from local regulation. However, on October 6, 2003, the 9th U.S. Appeals Court in San Francisco vacated the FCC's Declaratory Ruling that cable modem service is an exclusively "interstate information service." Subsequently on August 27, 2004, the FCC and the DOJ filed a joint petition with the US Supreme Court seeking to overturn the appeals court ruling; the Supreme Court has accepted the case (*National Cable and Telecommunications Association v. Brand X Internet Services*) and oral arguments were held on March 29, 2005.

Federal Assistance for Broadband Deployment

In the 109th Congress, legislation has been introduced to provide financial assistance (including loans, grants, and tax incentives) to encourage broadband deployment (H.R. 144, H.R. 146, S. 14, S. 497, S. 502). For more information on federal assistance for broadband deployment, see CRS Report RL30719, *Broadband and the Digital Divide: Federal Assistance Programs*.

Computer and Internet Security[11]

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

---

[11] By John D. Moteff, Resources, Science, and Industry Division.

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 previous 12 months has steadily declined over the last four years.[12]

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 series of denial-of-service attacks of February 2000[13]. 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 the majority of 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 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

---

[12] 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 April 11, 2005. A different survey conducted by CSO Magazine, in cooperation with the U.S. Secret Service, and CERT (*2004 E-Crime Watch Survey),* released in May 2004, 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.

[13] This refers to the series of attacks, in February 2000, directed at on-line giants Yahoo, eBay, Amazon, E Trade, DATEK, Excite, ZDNEt, buy.com, and CNN.

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*. The *Strategy* assigned a number of responsibilities for coordinating the protection of the nation's information infrastructure to the Department of Homeland Security. Most of the Department's efforts in cybersercurity are managed by the National Cyber Security Division (NCSD) within the Information Analysis and Infrastructure Protection Directorate. As part of the *Strategy*, the NCSD has assumed a major role in raising awareness of the risks associated with computer security among all users, from the home user to major corporations, and to facilitate information exchange between all parties. To this end numerous cooperative and coordinating groups and fora have been established. One such activity is U.S.-CERT, a cooperative effort by the National Cyber Security Division and Carnegie Mellon's CERT, which among other services and activities, produces alerts of new and existing attacks and guidelines for preventing or responding to them.

Congress has shown, and continues to show, a strong interest in the security of computers and the Internet. Over the years this interest has been manifested in numerous hearings by a multitude of committees and subcommittees, in both the House and the Senate. Legislation has also been passed. The federal Computer Fraud and Abuse statute (18 U.S.C. 1030) was initially added as part of the Comprehensive Crime Control Act of 1984 (P.L. 98-473). This act, as amended, makes it a federal crime to gain unauthorized access to, damage, or use in an illegal manner, protected computer systems (including federal computers, bank computers, and computers used in interstate and foreign commerce).[14] Legislation specifically requiring system owners/operators to take actions to protect their computer systems has been confined to executive federal agencies (most recently, the Federal Information Security Management Act of 2002, P.L. 107-347, Title III). Other legislation is primarily aimed at protecting privacy by protecting certain personal information held by government and private sector entities and affects computer security indirectly. For example, the Gramm-Leach-Bliley Act (P.L. 106-102, Title V) and the Health Insurance Portability and Accountability Act of 1996 (HIPPA, P.L. 104-191, Title II, Subtitle F) require that entities have in place programs that protect the financial and health-related information, respectively, in their possession. The Sarbannes-Oxley Act of 2002 (P.P. 107-204) also indirectly affects private sector computers and networks, by requiring certain firms to certify the integrity of their financial control systems as part of their annual financial reporting requirements. To the extent that this information resides on computer systems, these requirements extend to those systems. Congress also supports a number of programs that help develop computer security education, training, and research at selected universities. For an overview of federal legislation and other federal documents associated with computer and internet security, see CRS Report RL32357, *Computer Security: A Summary of Selected Federal Laws, Executive Orders, and Presidential Directives*.

It is not clear how these efforts have affected the overall security of the Internet. Given the perceived rise in security threats and attacks, there is a general sense that

---

[14] Some of the penalties under this statute were increased by both the U.S.A. PATRIOT Act (P.L. 107-56, Sec. 814) and the Homeland Security Act of 2002 (P.L. 107-296, Sec. 225(g)).

more must be done. Aside from the inherent vulnerabilities associated with highly interconnected information networks, two major sources of vulnerabilities exist: software, and network configuration and 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. Although patches typically are offered to fix these vulnerabilities, many system administrators do not keep their software/configurations current. Many intrusions take advantage of software vulnerabilities noted many months earlier, for which fixes have already been offered.

There are as yet no agreed upon 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 damage done to a third-party computer as a result of inadequately protecting their own systems.[15] Nor are there any agreed upon standards on how secure a vendor's software product 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. For a discussion of the difficulties associated with setting standards, see CRS Report RL32777, *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*.

So far in the 109th Congress, legislation has been introduced that again, primarily addresses privacy issues with indirect impact on computer security. In light of recent large losses of personal information through fraud, lost records, and unauthorized access, a number of bills have been introduced that extend the requirements to safeguard and protect personal information, as found in Gramm-Leach-Bliley and HIPPA, to "information brokers" (H.R. 1080, H.R. 1263, S. 500). In addition, bills have been introduced that require any organization engaged in interstate commerce which holds personal information to inform consumers of any security breach that may have compromised their information (H.R. 1069). Bills commonly referred to as "spyware" legislation have also been introduced (H.R. 29, HR. 744, and S. 687, discussed in the next section). Addressing a different issue, H.R. 285 would elevate cybersecurity within the Department of Homeland Security's bureaucracy by creating a position of Assistant Secretary for Cybersecurity within the Information Analysis and Infrastructure Protection Directorate.

---

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

Internet Privacy[16]

Internet privacy issues encompass a range of concerns. One is that the Internet makes it easier for government 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, or surreptitiously installed software ("spyware"), collect personally identifiable information (PII) and share that information with third parties, usually without the knowledge or consent of the people concerned. Another aspect 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.

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.

Commercial Websites. Although the FTC and the Clinton Administration favored self regulation, in 1998, frustrated at industry's slow pace, the FTC sought and Congress passed the Children's Online Privacy Protection Act (COPPA, part of P.L. 105-277). Many bills have been introduced since that time to extend protection to others, but the only ones that have passed involve federal government websites (see below). Industry has taken steps to demonstrate that it can self regulate. One example is the establishment of "seals" by groups such as the Better Business Bureau and TRUSTe. To display a seal, 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 these efforts 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. For the status of legislation pending in the 109th Congress, see CRS Report RL31408, *Internet Privacy: Overview and Pending Legislation*.

---

[16] By Marcia S. Smith, Resources, Science, and Industry Division. See also CRS Report RL31408, *Internet Privacy: Overview and Pending Legislation*, which is updated more frequently than this report.

Federal Websites. In June 2000, 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 has included provisions in the Treasury-General Government (or Treasury-Transportation) Appropriations Acts every year since FY2001 prohibiting agency from collecting, reviewing, or creating aggregate lists that include 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. Congress also passed the E-Government Act (P.L. 107-347) which requires federal websites to provide a privacy notice about their information practices, and to translate their privacy policies into a standardized machine-readable format, enabling P3P to work, for example.

Spyware

Spyware is another focus of congressional concern. There is no firm definition of spyware, but one example is software products that include a method by which information is collected about the use of the computer on which the software is installed, and the user. 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. Typically, users have no knowledge that the software they obtained included spyware and that it is now resident 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. Three bills — H.R. 29, H.R. 744, and S. 687 — are pending in the 109th Congress (see CRS Report RL32706, *Spyware: Background and Policy Issues for Congress*).

Identity Theft and "Phishing"

The growth in the number of cases of "identity theft," where one individual assumes the identity of another to commit fraud, is alarming to many consumers, including many Members of Congress. Despite widespread public perception that

the Internet is a major contributor to the rise in identity theft, surveys indicate that comparatively few individuals who know how a thief acquired their personally identifiable information (PII) cite the Internet. Some attribute the rise in identity theft instead to carelessness by businesses in handling PII, and by credit issuers that grant credit without proper checks.

The Internet may play a role, however. Today, attention is focused on a relatively new scam called "phishing." Phishing refers to a practice where someone misrepresents their identity or authority in order to induce another person to provide PII over the Internet. Some common phishing scams involve e-mails that purport to be from a financial institution, ISP, or other trusted company claiming that a person's record has been lost. The e-mail directs the person to a website that mimics the legitimate business' website and asks the person to enter a credit card number and other PII so the record can be restored. In fact, the e-mail or website is controlled by a third party who is attempting to extract information that will be used in identity theft or other crimes. The FTC issued a consumer alert on phishing in June 2004.[17]

Several laws restrict the disclosure of consumer information and require companies to ensure the security and integrity of the data in certain contexts — Section 5 of the Federal Trade Commission Act, the Fair Credit Reporting Act (FCRA), and Title V of the Gramm-Leach-Bliley Act. Congress also has passed several laws specifically related to identity theft: the 1998 Identity Theft and Assumption Deterrence Act; the 2003 Fair and Accurate Credit Transactions (FACT) Act; and the 2004 Identity Theft Penalty Enhancement Act. Those laws are summarized in CRS Report RL31919, *Remedies Available to Victims of Identity Theft*. At a March 10, 2005 Senate Banking Committee hearing, FTC Chairwoman Majoras referred to the "complicated maze" of laws that govern consumer data, based on the type of company or institution involved, the type of data collected or sold, and the purpose for which it will be used. A number of bills are pending the 109th Congress that are related to identity theft, and hearings have been held. See CRS Report RS22082, *Identity Theft: The Internet Connection*, for more on the role the Internet may play in this crime.

Monitoring of E-Mail and Web Activity

By Government and Law Enforcement Officials. In the summer of 2000, it became known that the FBI, with a court order, was installing software on ISP's 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. The reports were obtained by the Electronic Privacy Information Center (EPIC) through the Freedom of

---

[17] FTC. How Not to Get Hooked by a 'Phishing" Scam. June 2004. [http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.pdf]

Information Act in 2005. According to the reports, the FBI no longer uses Carnivore/DCS 1000, but uses commercially available software instead.

The overall environment for debating privacy issues changed substantially after the September 11, 2001, terrorist attacks. Congress passed the USA PATRIOT Act (P.L. 107-56), which expands the ability of government and law enforcement authorities to monitor Internet activities. The Internet privacy-related provisions of the USA PATRIOT Act are discussed in CRS Report RL31289, *The Internet and the USA PATRIOT Act: Potential Implications for Electronic Privacy, Security, Commerce, and Government*. One of the more controversial provisions is Section 212, which *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. As amended in 2002 (by section 225 of the Homeland Security Act), it also allows an ISP to divulge *the contents* of communications to a Federal, state, or local governmental entity if it has a good faith belief that an emergency involving danger of death or serious physical injury requires disclosure of the information without delay. The amended version of the language lowered the threshold for permitting ISPs to divulge contents. Privacy advocates are concerned about the revised language. EPIC notes, for example, that allowing an ISP to disclose the contents of a communication to any governmental entity (instead of a "law enforcement agency" as had been stated in the original Act) not only poses increased risk to personal privacy, but also is a poor security strategy.

Several of the Internet-related sections of the USA PATRIOT Act, including Sec. 212, are covered by a "sunset" clause under which they will expire on December 31, 2005. Legislation was introduced in the last Congress that would either have extended the sunset clause to additional sections, or abolished the sunset clause entirely. No bill passed, and the debate has resumed in the 109th Congress.

By Employers. Another issue is whether employers should be required to notify their employees if e-mail or other computer-based activities are monitored. 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, a U.S. Circuit Court of Appeals ruled in 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 an e-mail service provider that sold out-of-print books. The company 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 a competitor so company officials could read the e-mails and obtain a competitive advantage. 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.

"Spam": Unsolicited Commercial Electronic Mail[18]

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 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.

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. Skeptics counter that 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 how it is defined.

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 FCC to establish regulations to protect wireless consumers from spam. The FCC issued those rules in August 2004. See CRS Report RL31636, *Wireless*

---

[18] By Marcia S. Smith, Resources, Science, and Industry Division. See also CRS Report RL31953, "*Spam: An Overview of Issues Concerning Commercial Electronic Mail*," which is updated more frequently than this report.

Privacy and Spam: Issues for Congress, for more on wireless privacy and wireless spam.

Protecting Children from Unsuitable Material[19]

Preventing children from encountering unsuitable material, such as pornography, as they use the Web has been a major congressional concern for many years. Several laws have been passed. They are summarized in CRS Report RS21328, *Internet: Status of Legislative Attempts to Protect Children from Unsuitable Material on the Web*.

The laws include the 1996 Communications Decency Act (CDA), the 1998 Child Online Protection Act (COPA), and the 2000 Children's Internet Protection Act (CIPA). Federal courts ruled, in turn, that certain sections of CDA, COPA and CIPA were unconstitutional. All the decisions were appealed to the Supreme Court. The Supreme Court upheld the lower court decision on CDA in 1997. It heard COPA twice, in 2002 and 2004, and each time remanded the case to a lower court. The Supreme Court upheld CIPA in 2003. CIPA requires schools and libraries that receive federal funding to use filtering technologies to block minors' access to Web pages that contain material that is obscene, child pornography, or "harmful to minors" (as defined in CIPA). It also requires libraries receiving federal funds to block websites containing obscene material or child pornography from access by adults.

Congress also passed the "Dot Kids" Act (P.L. 107-317), which creates a kid friendly space on the Internet, and the "Amber Alert" Act (P.L. 108-21) which, inter alia, prohibits the use of misleading domain names to deceive a minor into viewing material that is harmful to minors.

Congressional attention on protecting children initially focused on the Web as the potential source of unsuitable material, but concern is rising about the availability of pornography on "peer-to-peer" (P2P) networks. These networks use file-sharing software to allow individual users to communicate directly with each other via computer, rather than accessing websites. Such file-sharing programs are perhaps best known because of their widespread use for downloading copyrighted music, raising concerns about copyright violations.[20] P2P networks can be used for sharing any type of files, however, not only music. A February 2003 GAO report found that "When searching and downloading images on peer-to-peer networks, juvenile users face a significant risk of inadvertent exposure to pornography, including child

---

[19] By Marcia S. Smith, Resources, Science, and Industry Division. See also CRS Report RS21328, *Internet: Status Report on Legislative Attempts to Protect Children from Unsuitable Material on the Web*, and CRS Report 95-804, *Obscenity and Indecency: Constitutional Principles and Federal Statutes*.

[20] For more on these issues, see CRS Report RL31998, File-Sharing Software and Copyright Infringement: Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.

pornography."[21] Then-Attorney General Ashcroft announced the results of a major law enforcement effort against P2P networks that distribute child pornography in May 2004.[22] Legislation was introduced, and hearings were held, in the last Congress, but no bill passed. Congressional interest in P2P networks is expected to continue in the 109th Congress.

Internet Domain Names[23]

The 109th Congress continues to monitor issues related to the Internet domain name system (DNS). Internet domain names were created to provide users with a simple location name for computers on the Internet, rather than using the more complex, unique Internet Protocol (IP) number that designates their specific location. As the Internet has grown, the method for allocating and designating domain names has become increasingly controversial.

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

---

[21] U.S. General Accounting Office. File-Sharing Programs: Peer-to-Peer Networks Provide Ready Access to Child Pornography. GAO-03-351. February 2003. p. 3. [http://www.gao.gov]

[22] Department of Justice. Departments of Justice, Homeland Security Announce Child Pornography File-Sharing Crackdown. Press release, May 14, 2004. [http://www.usdoj.gov/opa/pr/2004/May/04_crm_331.htm]

[23] By Lennard G. Kruger, Resources, Science, and Industry Division. See also CRS Report 97-868, *Internet Domain Names: Background and Policy Issues*, which is updated more frequently than this report.

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. 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. In the 109th Congress, the Senate Committee on Commerce, Science and Transportation and the House Committee on Energy and Commerce will likely conduct oversight on how the Administration manages and oversees ICANN's activities and policies as it strives to meet the conditions of the Department of Commerce MOU. The 109th Congress is also likely to assess the role of the federal government in Internet governance, the nature and implications of the transition of the DNS to private sector ownership, and the role that the international community might play in that transition.

Top Level Domains. At its July 16, 2000 meeting in Yokohama, Japan, 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. 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. On March 28, 2005, ICANN published an evaluation report identifying Verisign as the highest ranked applicant for operating the .net registry. ICANN says it will now enter into negotiations with Versign for operating the .net registry.

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 how to achieve greater international involvement in the governance of the Internet and the domain name system. The study is being conducted by the UN's Working Group on Internet Governance (WGIG). The United Nations will revisit the issue in November 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.

On March 31, 2005, the National Research Council (NRC) released a report entitled, *Signposts in Cyberspace: The Domain Name System and Internet Navigation*. The report was mandated by Congress in 1998 (P.L. 105-305) and sponsored by the DOC and NSF. Among its recommendations, the NRC concluded that the domain name system should continue to be administered by a nongovernmental body and not be turned over to an intergovernmental organization.

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, Chile, 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 $1,000) 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.

Privacy. Any entity who registers a domain name is required to provide contact information (phone number, address, email) which is entered into a public online database (the "WHOIS" database). Over the past several years, registrants who wish to maintain their privacy have been able to register anonymously using a proxy service offered by some registrars. In February 2005, the National Telecommunications and Information Administration (NTIA) — which has authority over the .us domain name — notified Neustar (the company that administers .us) that proxy or private domain registrations will no longer be allowed for .us domain name registrations, and that registrars must provide correct WHOIS information for all existing customers by January 26, 2006. According to NTIA, this action will provide an assurance of accuracy to the American public and to law enforcement officials. The NTIA policy is opposed by privacy groups and registrars (such as Go Daddy) who argue that the privacy, anonymity, and safety of people registering .us domain names will be needlessly compromised.

In a related development, in 2004, Congress passed the Fraudulent Online Identity Sanctions Act (Title II of the Intellectual Property Protection and Courts Amendments Act, 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.

Government Information Technology Management[24]

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

---

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

technology management issues focus on challenges faced by the FCC in regulating in the Internet era, on information technology research and development, on the provision of online services by the government ("e-government"), and on the availability and use of "open source" software.

The Federal Communications Commission[25]

The Federal Communications Commission (FCC), established by the 1934 Communications Act, regulates interstate and international communications by radio, television, wire, satellite, and cable. The FCC has had to continually adapt to ever-changing telecommunications technologies, policies, and services over those decades. The Internet age is another challenging milestone in the FCC's evolution. The agency must adhere to the statutory requirements of the 1934 Act, while "convergence" in the communications industry towards an all-digital, broadband world is blurring the distinctions between the services that the agency regulates. Convergence makes distinguishing among types of data increasingly difficult, while the FCC must differentiate among services based on distinctions drawn in 1934. When all data look the same, and functionally similar services are provided by companies governed by different titles of the 1934 Act, questions of fairness and competitive advantage may arise. As newer technologies and services are developed and deployed, applying legacy regulations to them may become more strained.

The FCC plans to address two issues directly related to convergence during the 109th Congress: the proper regulatory classification of services via the Internet protocol (e.g., Voice over Internet Protocol [VoIP]), and law enforcement's ability to conduct wiretaps effectively under the Communications Assistance for Law Enforcement Act (CALEA). These issues are considered particularly important because, as the FCC addresses them, a new regulatory environment for telecommunications and information services may be created.

The FCC is also expected to remain focused on broadband deployment issues (discussed earlier). Policies may be promulgated to encourage new providers to roll out new services (such as Broadband over Powerlines — BPL[26]), and to continue to promote broadband deployment to underserved areas and populations, such as rural and low-income communities, through universal service and other programs (e.g., the E-Rate).

One of the difficulties in addressing the issues facing the FCC is that so many of them intersect. Many of the broadband issues are so inter-related that it is often difficult to distinguish where one issue ends and another begins. For example, VoIP, CALEA, and BPL are all tied to the concept of broadband convergence and reliance

---

[25] By Patricia Moloney Figliola, Resources, Science, and Industry Division. For more information, see CRS Report RL32589, *The Federal Communications Commission: Current Structure and its Role in the Changing Telecommunications Landscape*, and CRS Issue Brief IB10045: *Broadband Internet Access: Background and Issues*, which are updated more frequently than this report.

[26] For more information, see CRS Report RS32421, *Broadband over Powerlines: Regulatory and Policy Issues*.

on the Internet for information. It becomes difficult, if not impossible, to discuss one without touching on the others. Effectively addressing these types of issues may well be the greatest challenge facing the FCC in the near future.

Information Technology R&D[27]

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 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 FY2006, the President requested a budget of $2.155 billion for the NITRD program, a 4.5% decrease from the FY2005 budget of $2.256 billion. (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 Congress 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 defining the private sector's role in this initiative.

Electronic Government (E-Government)[28]

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

---

[27] By Patricia Moloney Figliola, Resources, Science, and Industry Division. See also CRS Issue Brief IB10130, *The Federal Networking and Information Technology Research and Development Program; Funding Issues and Activities*, which is updated more frequently than this report.

[28] By Jeffrey W. Seifert, Resources, Science, and Industry Division. See also CRS Report RL31057, *A Primer on E-Government: Sectors, Stages, Opportunities, and Challenges of Online Governance*, which is updated more frequently than this report.

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 (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.[29] 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

---

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

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.

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 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[30]

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.

---

[30] By Jeffrey W. Seifert, Resources, Science, and Industry Division. See also CRS Report RL31627, *Computer Software and Open Source Issues: A Primer.*

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.

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 Pending Legislation

Following is a list of legislation pending before the 109th Congress on the topics covered in this report. The format is: bill number, sponsor, title, date introduced, and committee(s) of referral. This report does not track the legislative status of the pending legislation. For more information, see the CRS reports cited in the text of the relevant section of this report (and in Appendix D).

Broadband Internet Access

H.R. 144, McHugh, Rural America Digital Accessibility Act, 1/4/05 (Energy & Commerce, Ways & Means)
H.R. 146, McHugh, "to establish a grant program to support broadband-based economic development efforts," 1/4/05 (Transportation &Infrastructure, Financial Services)
H.R. 1479, Udall, Rural Access to Broadband Services Act, 4/5/05 (Ways & Means, Science, Energy & Commerce)

S. 14, Stabenow, Fair Wage, Competition, and Investment Act of 2005, 1/24/05 (Finance)
S. 497, Salazar, Broadband Rural Revitalization Act of 2005, 3/2/05 (Finance)
S. 502, Coleman, Rural Renaissance Act, 3/3/05 (Finance)

Internet Privacy

General

H.R. 84, Frelinghuysen, Online Privacy Protection Act, 1/4/05 (Energy & Commerce)
H.R. 1263, Stearns, Consumer Privacy Protection Act, 3/10/05 (Energy & Commerce, International Relations)

Spyware

H.R. 29, Bono, Spy Act, 1/4/05 (Energy & Commerce)
H.R. 744, Goodlatte, I-SPY Act, 2/10/05 (Judiciary)

S. 687, Burns, SPY BLOCK Act, 3/20/05 (Commerce)

Identity Theft and Related Topics

H.R. 82, Frelinghuysen, Social Security On-line Privacy Protection Act, 1/4/05 (Energy & Commerce)
H.R. 92, Frelinghuysen, to permit people to use an identification number other than a Social Security number for Medicare to deter identity theft, 1/4/05 (Ways & Means)
H.R. 220, Paul, Identity Theft Prevention Act, 1/4/05 (Ways & Means, Government Reform)

H.R. 1069, Bean, Notification of Risk to Personal Data Act, 3/3/05 (Energy & Commerce, Gov Reform, Financial Services)
H.R. 1078, Markey, Social Security Number Protection Act, 3/3/05 (Energy & Commerce, Ways &Means)
H.R. 1080, Markey, Information Protection and Security Act, 3/3/05 (Energy & Commerce)
H.R. 1099, Hooley, Anti-Phishing Act, 3/3/05 (Judiciary)

S. 29, Feinstein, Social Security Misuse Prevention Act, 1/24/05 (Judiciary)
S. 115, Feinstein, Notification of Risk to Personal Data Act, 1/24/05 (Judiciary)
S. 116, Feinstein, Privacy Act of 2005, 1/24/05 (Judiciary)
S. 472, Leahy, Anti-Phishing Act, 2/28/05 (Judiciary)
S. 500, Bill Nelson, Information Protection and Security Act, 3/3/05 (Commerce)

Government IT

H.R. 214, Stearns, Advanced Internet Communications Services Act, 1/4/2005 (Energy & Commerce)
H.R. 28, Biggert, High-Performance Computing Revitalization Act, 1/4/2005; approved by committee 3/17/2005 (Science)

Appendix B: List of Acronyms

Alphabetical Listing

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
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	Government Accountability Office (formerly 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 (part of Department of Commerce)
NSI	Network Solutions, Inc,
NSF	National Science Foundation
NTIA	National Telecommunications and Information Administration (part of Department of Commerce)
OMB	Office of Management and Budget
OPA	Online Privacy Alliance
OSS	Open Source Software
SSN	Social Security Number
TLD	Top Level Domain
UCE	Unsolicited Commercial E-mail
WIPO	World Intellectual Property Organization

Categorical Listing

U.S. Government Entities	
DOC	Department of Commerce
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FTC	Federal Trade Commission
GAO	Government Accountability Office (formerly General Accounting Office)
GSA	General 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)
OMB	Office of Management and Budget
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.
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	
MOU	Memorandum of Understanding
SSN	Social Security Number
WIPO	World Intellectual Property Organization

Appendix C: Legislation Passed by the 105th - 108th Congresses

During the years that this report has been published (since the 105th Congress), various topics have been covered based on congressional interest and action. 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, and therefore are not discussed in the main text. Nevertheless, it appears useful to retain information about legislation that passed on those subjects. Following is such a summary of all laws that have been tracked in this report over the years, by topic. Tables showing which laws were passed in each Congress appear at the end of this section.

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.

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.

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 (Including Identity Theft)

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.

Language in the **FY2001 Transportation Appropriations Act (P.L. 106-246)** and the **FY2001 Treasury-General Government Appropriations Act** (included as part of the FY2001 Consolidated Appropriations Act, P.L. 106-554) addresses website information collection practices by departments and agencies. 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 **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.

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.

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

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 (Section 1061), 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.

Spam: Unsolicited Commercial E-Mail

The **CAN-SPAM Act, P.L. 108-187**, 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.

Internet Domain Names

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.

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.

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.

The **PROTECT Act (P.L. 108-21)** 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** (Title II of the Intellectual Property Protection and Courts Amendments Act of 2004, **P.L. 108-482**) 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.

Protecting Children from Unsuitable Material and Predators on the Internet

The **Child Online Protection Act**, Title XIV of Division C of the FY1999 Omnibus Appropriations Act, **P.L. 105-277**), made it a crime to send material over the Web that is "harmful to minors" to children. Similar language was also included in the Internet Tax Freedom Act (Title XI of Division C of the same 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 restricted access to commercial material that is "harmful to minors" distributed on the World Wide Web to those 17 and older. This act also was challenged in the courts. See CRS Report 98-670 for a summary of court actions.

The **Children's Online Privacy Protection Act** (Title XIII of Division C of the FY1999 Omnibus Appropriations Act, **P.L. 105-277**), requires verifiable parental consent for the collection, use, or dissemination of personally identifiable information from children under 13.

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.

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.

E-Government

The **E-Government Act of 2002 (P.L. 107-347)** 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).

Intellectual Property

Congress passed the **Digital Millennium Copyright Act (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*).

Electronic and Digital Signatures

The **Government Paperwork Elimination Act** (Title XVII of Division C of the Omnibus Appropriations Act, **P.L. 105-277**)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.

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.

Electronic Commerce

The **Internet Tax Nondiscrimination Act (P.L. 107-75)** extended the Internet tax moratorium through November 1, 2003. Facing expiration of that moratorium, Congress passed the **Internet Tax Non-Discrimination Act of 2003 (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.

Table 1: 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

Table 2: Summary of Legislation Passed by 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
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

Table 3. Summary of Legislation Passed by the 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

Table 4: Summary of Legislation Passed by the 108th Congress

Title	Public Law Number
PROTECT Act (Section 108, Misleading Domain Names on the Internet)	P.L. 108-21
CAN-SPAM Act	P.L. 108-187
Internet Tax Non-Discrimination Act of 2003	P.L. 108-435
Intelligence Reform and Terrorism Protection Act (Section 1061)	P.L. 108-458
Fraudulent Online Identity Sanctions Act (Title II of the Intellectual Property Protection and Courts Amendments Act of 2004)	P.L. 108-482
Commercial Spectrum Enhancement Act (Title II of the ENHANCE 911 Act)	P.L. 108-494

Appendix D: Related CRS Reports

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 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.

Computer and Internet Security

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

CRS Report RL32777. *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*, by Eric A. Fischer

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.

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

CRS Report RS22078. *Privacy and Civil Liberties Oversight Board: 109th Congress Proposed Refinements*, by Harold C. Relyea.

CRS Report RS21851. *Privacy Protection: Mandating New Arrangements to Implement and Assess Federal Privacy Policy and Practice*, by Harold C. Relyea.

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

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

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

"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.

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.

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 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: A Brief 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 in the 107th and 108th Congresses*, by Robin Jeweler.

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

Electronic Commerce

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

CRS Report RL31929. *Internet Taxation: Issues and Legislation*, 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. *State and Local Sales and Use Taxes and Internet Commerce*, by Stephen Maguire.

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

Identity Theft

CRS Report RS22082. *Identity Theft: The Internet Connection*, by Marcia S. Smith.

CRS Report RL32535. *Implementation of the Fair and Accurate Credit Transactions (FACT) Act of 2003*, by Angie A. Welborn and Grace Chu.

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

Medical Records, Financial, and Other Privacy Issues

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.

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.