Order Code 98-67

CRS Report for Congress

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

Updated January 5, 2007

Lennard G. Kruger, John D. Moteff, Angele A. Gilroy,
Jeffrey W. Seifert, and Patricia Moloney Figliola
Resources, Science, and Industry Division

Rita Tehan
Knowledge Services Group

Prepared for Members and
Committees of Congress

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 63%, and by 2005, stood at 78.6%. From electronic mail to accessing information to watching videos to online purchasing, 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 "dial-up" 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"), protecting children from unsuitable material (such as pornography), and computer security, including the vulnerability of the nation's critical infrastructures to cyber attacks.

Other issues include the Internet's domain name system (DNS), which is administered by a nonprofit corporation called the Internet Corporation for Assigned Names and Numbers (ICANN). With the Department of Commerce currently exercising legal authority over ICANN, Congress continues to monitor the administration of the DNS, particularly with respect to issues such as privacy, governance, and protecting children on the Internet.

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. Other CRS reports referenced in this document track legislation, and the reader should consult those reports, which are updated more frequently than this one, for current information.

This report will not be updated.

Contents

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

Introduction

The continued growth of the Internet for personal, government, and business purposes may be affected by a number of technology policy issues being debated by Congress. Among them are access to and regulation of 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 acronyms, and a discussion of legislation passed in earlier Congresses. Other issues that are not directly related to technology could also affect the use and growth of the Internet, such as intellectual property rights and Internet taxation. Those are not addressed in this report.

This report does not attempt to track legislation. For more timely information, see the other CRS reports identified in the following sections.

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

A December 2006 survey by the Nielsen/Net Ratings market research firm found that 78% of active home Web users connected via broadband during the month of November, up 13 percentage points from 65% of active Web users a year ago. Social activities dominate broadband time online: websites for online gaming, instant messaging, e-mail and social networking all made the top 10 list when ranked by average time per person among broadband users at home. The Internet has become an integral part of everyday social life, particularly among children and teenagers.[2]

---

[1] By Rita Tehan, Knowledge Services Group.

[2] Nielsen/NetRatings press release, *Over Three-fourths of U.S. Active Internet Users Connect via Broadband at Home in November, According to Nielsen/Netratings*, December 12, 2006. See [http://www.nielsen-netratings.com/pr/pr_061212.pdf].

A spring 2006 Pew Internet & American Life survey found that 48 million Americans — mostly those with high-speed access at home — have posted content to the Internet.[3]

Internet Usage in the United States

Trends. The *Fifth Study of the Internet by the Digital Future Project Finds Major New Trends in Online Use for Political Campaigns*[4] highlights the major findings in the Annenberg School's Digital Future Project, which is studying the impact of the Internet on Americans. Among the findings are:

- Internet users are finding growing numbers of online friends, as well as friends they first met online and then met in person. Internet users report having met an average of 4.65 friends online whom they have never met in person.
- Although more than 40%of users say that the Internet has increased the number of people with whom they stay in contact, a lower percent say that since starting to use the Internet they are communicating more with family and friends.
- While large percentages of Internet users say that going online increases contact with family and friends, almost all users report that the Internet has no effect on the time spent with close friends or family face-to-face.

Number of Users. The Federal Communications Commission (FCC) issues biannual reports on broadband Internet access service.[5] In its July 2006 report, the FCC reported that during the year 2005, high-speed lines serving residential, small business, larger business, and other subscribers increased by 33%, to 50.2 million lines. High-speed lines serving residential and small business subscribers increased by 36% during 2005, to 42.9 million lines.[6] Additional demographic information on Internet users is compiled by MRI Cyberstats.[7]

Geographic Distribution. Rural Americans are less likely to log on to the Internet at home with high-speed Internet connections than people living in other

---

[3] Pew Internet and American Life. *Home Broadband Adoption 2006*, May 28, 2006. See [http://www.pewinternet.org/PPF/r/184/report_display.asp].

[4] USC Annenberg School, Center for the Digital Future. *Online World As Important to Internet Users as Real World?*, November 29, 2006. See [http://www.digitalcenter.org/pages/news_content.asp?intGlobalId=212&intTypeId=1].

[5] 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.

[6] FCC. Federal Communications Commission Releases Data on High-Speed Services for Internet Access. Press release, July 26, 2006. Available at [http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-266593A1.pdf].

[7] MRI Cyberstats, *Internet Access and Usage in the U.S.*, Spring 2006. See [http://www.infoplease.com/ipa/A0908398.html]

parts of the country. However, rural areas show fast growth in home broadband uptake in the past two years and the gap between rural and non-rural America in home broadband adoption, though still substantial, is narrowing. As of March 2006, 39% of adult rural Americans went online at home with high-speed Internet connections compared with 42% of adults in urban and suburban areas.[8] *A Nation Online: Entering the Broadband Age*, the sixth report released by the U.S. Department of Commerce examining Americans' use of computers, the Internet, and other information technology tools, examined the geographic differences in broadband adoption and the reasons why some Americans do not have high-speed service.[9] According to the 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

There are many different estimates of international Internet usage. Some sources which compile Internet usage data are: the International Telecommunications Union (ITU), the Organisation for Economic Co-operation and Development (OECD), the CIA Fact Book, and independent market research firms such as Nielsen//NetRatings, eMarketer, and the Computer Industry Almanac.[10]

According to a January 2006 estimate from the Computer Industry Almanac, the worldwide number of Internet users is 1.08 billion.[11] The 2 billion Internet users milestone is expected to occur in 2011. Much of current and future Internet user growth is coming from highly populated countries such as China, India, Brazil, Russia, and Indonesia. In the next decade many Internet users will be accessing the Internet with mobile devices, in addition to personal computers.[12]

Broadband subscribers in the Organisation for Economic Cooperation and Development (OECD) member countries[13] reached 181 million by June 2006. Over

---

[8] Pew Internet & American Life, *Home Broadband Adoption 2006*, May 28, 2006. See [http://www.pewinternet.org/PPF/r/176/report_display.asp].

[9] U.S. Department of Commerce. A Nation Online: Entering the Broadband Age. September 2004. See [http://www.ntia.doc.gov/reports/anol/index.html]. Rural/urban geographic distribution figures are on pp. 15-19.

[10] One source of comparative data is: *Internet Usage Statistics - The Big Picture World Internet Users and Population Stats*. See [http://internetworldstats.com/stats.htm].

[11] ClickZ Stats, *Web Worldwide*, See: [http://www.clickz.com/showPage.html?page=stats/web_worldwide].

[12] Computer Industry Almanac, *Worldwide Internet Users Top 1 Billion in 2005*, January 4, 2006. See [http://www.c-i-a.com/pr0106.htm].

[13] OECD member countries include include Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, The Netherlands, New Zealand, Norway, Poland, Portugal, Slovak Republic, Spain, Sweden, Switzerland, Turkey, United Kingdom, and the

(continued...)

the past year, the number of broadband subscribers in the OECD increased 33% from 136 million in June 2005 to 181 million in June 2006. This growth increased broadband penetration rates in the OECD from 11.7 in June 2005 to 15.5 subscriptions per 100 inhabitants one year later.[14] The main highlights for the first half of 2006 are:

- Northern European countries have continued their advance with high broadband penetration rates. In June 2006, six countries (Denmark, the Netherlands, Iceland, Korea, Switzerland and Finland) led the OECD in broadband penetration, each with at least 25 subscribers per 100 inhabitants.
- Denmark now leads the OECD with a broadband penetration rate of 29.3 subscribers per 100 inhabitants.
- The strongest per-capita subscriber growth comes from Denmark, Australia, Norway, the Netherlands, Finland, Luxembourg, Sweden and the United Kingdom.
- The United States has the largest total number of broadband subscribers in the OECD at 57 million representing 31% of all broadband connections in the OECD.

E-Commerce

The U.S. Census Bureau releases quarterly retail e-commerce statistics. On November 17, 2006, its estimate of U.S. retail e-commerce sales for the third quarter of 2006, adjusted for seasonal variation and holiday and trading-day differences, but not for price changes, was $27.5 billion, an increase of 4.5% from the 2nd quarter of 2006. Total retail sales for the 4th quarter of 2006 were estimated at $991.7 billion, an increase of 0.7% from the 2nd quarter of 2006.[15] E-commerce sales in the third quarter accounted for 2.8% of total sales.

ComScore Networks reported its e-commerce sales estimates for the first three quarters of 2006 and forecasts for the entire year. Overall, comScore forecasts that total online spending in 2006 will reach approximately $170 billion. Of that total, the market research firm estimates that non-travel e-commerce will break the $100 billion threshold for the first time. Through the first three quarters of 2006, total e-commerce spending rose 19 percent versus last year to $122.1 billion, buoyed by a 24% increase in non-travel spending to $69.1 billion.[16]

---

[13] (...continued)
United States.

[14] OECD Broadband Statistics to June, 2006. See [http://www.oecd.org/sti/ict/broadband].

[15] U.S. Census Bureau. *Quarterly Retail E-commerce Sales, 1st quarter 2006*, May 18, 2006. See [http://www.census.gov/mrts/www/ecomm.html].

[16] comScore press release, "U.S. Non-Travel E-Commerce Spending By Consumers Increased 23 Percent in Q3 2006 Versus Year Ago, According to comScore Networks," October 26, 2006. See [http://www.comscore.com/press/release.asp?press=959].

Broadband Internet Regulation and Access[17]

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. Broadband technologies — cable modem, digital subscriber line (DSL), satellite, wireless Internet, and fiber — are currently being deployed nationwide by the private sector. While the numbers of new broadband subscribers continue to grow, some areas of the nation — particularly rural and low-income communities — continue to lack sufficient access to high-speed broadband Internet service. In order to address this problem, the 109th Congress considered, but did not pass, legislation to address the scope and effect of federal broadband financial assistance programs (including universal service), and the impact of regulatory policies and new technologies on broadband deployment. These issues are anticipated to continue to be a focus of the broadband policy debate in the 110th Congress.

Some policymakers, believing that disparities in broadband access across American society could have adverse economic and social consequences on those left behind, assert that the federal government should play a more active role to avoid a "digital divide" in broadband access. One approach is for the federal government to provide financial assistance to support broadband deployment in underserved areas. In the 109th Congress, legislation was introduced, but not enacted, to provide financial assistance (including loans, grants, and tax incentives) to encourage broadband deployment. (For more information on federal assistance for broadband deployment, see CRS Report RL30719, *Broadband Internet Access and the Digital Divide: Federal Assistance Programs*, by Lennard G. Kruger and Angele A. Gilroy.) Others, however, question the reality of the "digital divide," and argue that federal intervention in the broadband marketplace would be premature and, in some cases, counterproductive.

The debate over access to broadband services has prompted policymakers to examine a range of other issues to ensure that broadband will be available on a timely and equal basis to all U.S. citizens. One facet of this debate focuses on whether present laws and subsequent regulatory policies are needed to ensure the development of competition and its subsequent consumer benefits, or conversely, whether such laws and regulations are overly burdensome and discourage needed investment in and deployment of broadband services. The regulatory debate focuses on a number of issues including the extent to which legacy regulations should be applied to traditional providers as they enter new markets, the extent to which legacy regulations should be imposed on new entrants as they compete with traditional providers in their markets, and the treatment of new and converging technologies.

For example, present law requires all incumbent local exchange (telephone) carriers (ILECs), such as Verizon or SBC, to open up their networks to enable competitors to lease out parts of the incumbent's network. These unbundling and

---

[17] By Angele A. Gilroy and Lennard G. Kruger, Resources, Science, and Industry Division. See also CRS Report RL33542, *Broadband Internet Regulation and Access: Background and Issues*, by Angele A. Gilroy and Lennard G. Kruger, which is updated more frequently than this report.

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. Whether such "open access" regulations should be applied to ILECs when they offer new non-dominant services such as broadband connections, or to new market entrants such as cable television companies when they offer services (such as voice and broadband) remains under debate. Whether regulators should play a role to ensure that the Internet remains open to all, often referred to as "net neutrality" became a major part of and is expected to continue to be, a major focus of the ongoing Congressional debate. Equally contentious is the debate over whether legacy regulations, such as the requirement that cable television companies obtain a local franchise as a prerequisite for offering video service, be extended to other entrants, such as telephone companies, if they choose to enter the video market. A third and related debate surrounds the appropriate regulatory framework that should be imposed on new technologies such as voice over Internet Protocol (VoIP) and other Internet Protocol services as well as bundled service offerings.

The regulatory treatment of broadband technologies — whether offered by traditional or emerging providers, or incumbent or new entrants — remains a major focus of the policy debate. 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. 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. After a series of conflicting court decisions the US Supreme Court in a June 27, 2005 action (*National Cable and Telecommunications Association v. Brand X Internet Services*), ruled that the FCC should be given deference in its decision that cable broadband service should be classified as an "interstate information service." The classification of cable modem service as an "interstate information service" will result in FCC treatment under the less rigorous Title I of the 1934 Communications Act. Similarly, in an August 5, 2005 action, the FCC ruled that the regulatory treatment of wireline broadband services will be granted regulatory parity. The FCC ruled that, subject to a one-year transition period, which expired in August 2006, wireline broadband Internet access services (commonly delivered by DSL technology) are defined as information services, thereby placing telephone company DSL services on an equal regulatory footing with cable modem services. Regulatory parity was also granted to broadband over power line (BPL) service, when the FCC, in a November 2006 decision, determined that such service would also be classified as an "interstate information service" subject to Title I regulation.

Finally, emerging broadband technologies — such as fiber, wireless (including "3G", "wi-fi" and "Wimax"), and BPL — continue to be developed and/or deployed, and have the potential to affect the regulatory and market landscape of broadband deployment. The 110th Congress and the FCC will likely consider policies to address the emergence of these and other new broadband technologies. In addition, how and to what extent "social regulations" such as 911 requirements, disability access, law enforcement obligations, and universal service support, should be applied to emerging technologies is also under debate. A related issue, the emergence of

municipal broadband networks (primarily wireless and fiber based) and the debate over whether such networks constitute unfair competition with the private sector has become a significant policy issue (for more information on municipal broadband, see CRS Report RS20993, *Wireless Technology and Spectrum Demand: Advanced Wireless Services*, by Linda K. Moore).

Computer and Internet Security[18]

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. Melissa virus, the Love Bug, and the Code Red, Nimda, Slammer, and Blaster worms) represents the tip of the iceberg. More recently, hackers using Trojan horses and other techniques, were able to place keylogging software on the personal computers of people with online trading accounts to surreptitiously acquire their personal account information. The hackers used the information to access these personal accounts to buy little known stocks in which they (the hackers) had invested, driving up the price. The thieves then dumped their shares for a profit.[19] Every day, persons gain access, or try to gain access, to someone else's computer without authorization to read, copy, modify, or destroy the information contained within. These persons range from juveniles to disgruntled (ex)employees, to criminals, to competitors, to politically or socially motivated groups, to agents of foreign governments.

The extent of the problem is unknown. Much of what gets reported as computer "attacks" are probes, often conducted automatically with software widely available for even juveniles to use. But the number of instances where someone has actually gained unauthorized access is not known. Not every person or company whose computer system has been compromised reports it either to the media or to authorities. Sometimes the victim judges the incident not to be worth the trouble. Sometimes the victim may judge that the adverse publicity would be worse. Sometimes the affected parties do not even know their systems have been compromised. There is some evidence to suggest, however, that the number of incidents is increasing. According to the Computer Emergency Response Team (CERT) at Carnegie-Mellon University, the number of incidents reported to it has grown just about every year since the team's establishment — from 132 incidents in 1989 to over 137,000 incidents in 2003. Since many attacks are now coordinated and cascade throughout the Internet, CERT no longer tracks the number of incidents reported to them. While the total number of incidents may be rising exponentially, it is interesting to note that, according to the Computer Crime and Security Survey,

---

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

[19] See, Computerworld. ID Thefts Slam Online Brokers, by Eric Lai. Vol. 40. No. 44. Oct. 30, 2006. p.1,43.

the percentage of respondents that reported unauthorized use of their computer systems over the previous 12 months has declined since the year 2000.[20]

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.[21] 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 2005 Computer Crime and Security Survey, 687 responders (out of a total of 700) estimated financial losses totaling $130 million in the previous 12 months. According to the survey, viruses accounted for the most financial losses ($43 million), followed by loss of proprietary information. Denial of service attacks accounted for $7 million in losses. Two of the online brokers whose customers' accounts were used in the "pump-and-dump" scheme mentioned above reported spending $22 million to compensate their customers.[22] 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*, by Brian Cashell, Will D. Jackson, Mark Jickling, and Baird Webel.

Aside from the losses discussed above, there is also growing concern that unauthorized access to computer systems could pose an overall national security risk should it result in the disruption of the nation's critical infrastructures (e.g., transportation systems, banking and finance, electric power generation and distribution). These infrastructures rely increasingly on computer networks to operate, and are themselves linked by computer and communication networks. In February 2003, the President's Critical Infrastructure Board (established by President George W. Bush through E.O. 13231 but later dissolved by E.O. 13286) released a *National Strategy to Secure Cyberspace*. The *Strategy* assigned a number of

---

[20] 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 2005 Survey indicated a slight increase, after four straight years of decline. Still over 50% of the respondents have reported unauthorized use. 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 July 10, 2006.

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

[22] Computerworld. Op. cit.

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 in the Preparedness 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, computers used in interstate and foreign commerce).[23] 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 Sarbanes-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*, by John Moteff.

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 more must be done. Aside from the inherent vulnerabilities associated with highly interconnected information networks, two major sources of vulnerabilities exist:

---

[23] Some of the penalties under this statute have been increased by both the USA PATRIOT Act (P.L. 107-56, Section 814) and the Homeland Security Act of 2002 (P.L. 107-296, Sectiom 225(g)).

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.[24] 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*, by Eric A. Fischer.

During the 109th Congress, legislation was introduced that, again, primarily addressed privacy issues with indirect impact on computer security. In light of large losses of personal information through fraud, lost records, and unauthorized access, a number of bills were introduced that extended the requirements to safeguard and protect personal information, similar to that found in Gramm-Leach-Bliley and HIPPA, to "information brokers" and/or required any organization engaged in interstate commerce holding personal information to inform consumers of any security breach that may have compromised their information. Bills commonly referred to as "Spyware" legislation were also introduced. These topics are discussed in the next section of this report. The theft of a laptop computer from the home of a employee of the Department of Veterans Affairs in May 2006, containing personal information of over 20 million military veterans, while not an Internet-related incident, renewed focus on the ability of federal agencies to enforce their own information security policies and procedures and to hold agency officials accountable. Such concern led the House to pass the Veterans Identity and Credit Security Act of 2006 (H.R. 5835) that included amendments to the Federal

---

[24] See "IT Security Destined for the Courtroom," *Computerworld*, May 21, 2001, vol. 35, no. 21, pp. 1, 73.

Information Security Management Act. The Senate did not take up the bill. Similar activity is expected in the 110th Congress.

Internet Privacy

Concerns related to Internet privacy encompass a wide range of issues. At the center of these issues is how networks can facilitate the collection and transfer of data inexpensively and on a large scale. While such data transfers can improve the efficiency and effectiveness of services, they can also pose great risk if the information is not appropriately protected. One example is the surreptitious installation of software ("spyware") by website operators to collect personally identifiable information (PII) and share that information with third parties, usually without the knowledge or consent of the people concerned. Another example is identity theft, which is a form of fraud in which the personal identifying information of an individual, such as a Social Security number, name, or date of birth, is co-opted by another person to facilitate committing a criminal or fraudulent act by impersonating the victim.

Spyware[25]

Spyware is another focus of congressional concern. There is no firm definition of spyware, but the most common 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. Most recently, the 109th Congress passed the Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2005 (US SAFE WEB) (P.L. 109-455). The bill allows the FTC and parallel foreign law enforcement agencies to share information while investigating allegations of "unfair and deceptive practices" that involve foreign commerce.

Identity Theft and "Phishing"[26]

Identity theft is a form of fraud in which the personal identifying information of an individual, such as a Social Security number, name, or date of birth, is co-opted by another person to facilitate committing a criminal or fraudulent act by impersonating the victim. Identity theft, also sometimes referred to as identity fraud, does not usually occur as a stand-alone crime. Instead, identity theft is often committed as part of some other fraud or white-collar crime, such as illegally

---

[25] By Patricia Moloney Figliola, Resources, Science, and Industry Division.

[26] By Jeffrey W. Seifert, Resources, Science, and Industry Division.

obtaining credit, taking over existing financial accounts, or establishing cellular phone service in the victim's name. An identity thief could also take other actions on behalf of the victim, such as establishing residency/citizenship, securing employment, obtaining government benefits, and committing other crimes in the victim's name. In addition, identity theft can play a facilitating role in potentially more violent crimes such as drug trafficking, people smuggling, and international terrorism.[27]

While identity theft is not solely an Internet issue, a number of high profile data breaches involving the personally identifiable information (PII) of citizens and consumers has drawn significant attention to the issue. Among the most recent incidents was the theft of a laptop containing the names, dates of birth, and other information of more than 26 million veterans. Although the laptop was eventually recovered and it is believed that the data was not accessed, the incident highlighted the ease with which the PII of large numbers of people could be taken at one time.

Another way identity theft can happen is through "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.[28]

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*, by Angie A. Welborn. For information on state laws and pending federal legislation, see CRS Report RS22484, *Identity Theft Laws: State Penalties and Remedies and Pending Federal Bills*, by Kristin Thornblad.

---

[27] General Accounting Office, *Identity Fraud: Prevalence and Links to Alien Illegal Activities*, GAO-02-830T, 25 June 2002, p. 10.

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

"Spam": Unsolicited Commercial Electronic Mail[29]

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. Although consumers are most familiar with spam on their personal computers, it also is becoming an issue in text messaging on wireless telephones and personal digital assistants (PDAs).

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 law 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 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. Additionally, the CAN-SPAM Act included a provision requiring the FCC to establish regulations to protect wireless consumers from spam.[30]

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.

---

[29] By Patricia Moloney Figliola, Resources, Science, and Industry Division. See also CRS Report RL31953, *Spam: An Overview of Issues Concerning Commercial Electronic Mail*, by Patricia Moloney Figliola, which is updated more frequently than this report.

[30] The FCC issued those rules in August 2004. See also CRS Report RL31636, *Wireless Privacy and Spam: Issues for Congress*, by Patricia Moloney Figliola, for more on wireless privacy and wireless spam.

In December 2005, the FTC submitted a report to Congress, as required under the CAN-SPAM Act, on the act's effectiveness and enforcement, and whether any changes are needed.[31] Based on information from ISPs, the general public, e-marketers, law enforcers, and technologists, the report concluded that the act has been effective in two areas: legitimate online marketers have adopted the "best practices" mandated by the act, and the act provides an additional tool for law enforcement officials and ISPs to bring suits against spammers. However, it also concluded that some aspects of the spam problem have not changed, such as its international dimension. It also reported on a number of "troubling" changes in the e-mail landscape, such as the inclusion of malicious content ("malware") in spam messages. The report outlined three steps to further improve the effectiveness of the act: passage of legislation to improve the FTC's ability to trace spammers and sellers who operate outside U.S. borders; continued consumer education; and continued improvement in anti-spam technologies, especially domain-level authentication.

Most recently, the 109th Congress passed the Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2005 (US SAFE WEB) (P.L. 109-455). The bill allows the FTC and parallel foreign law enforcement agencies to share information while investigating allegations of "unfair and deceptive practices" that involve foreign commerce, but raised some privacy concerns because the FTC would not be required to make public any of the information it obtained through foreign sources.

Protecting Children from Unsuitable Material[32]

Preventing children from encountering unsuitable material as they use the Web has been a major congressional concern for many years.[33] In response to this concern, Congress has passed such laws as the 1996 Communications Decency Act (CDA), the 1998 Child Online Protection Act (COPA), and the 2000 Children's Internet Protection Act (CIPA), all of which dealt in some way with the content found on the Internet. More recently, however, additional attention has been given to protecting children from exploitation and predators on the Internet. For example, in the last few years, social networking sites, such as MySpace, have become popular with teenagers and young adults. Unfortunately, there have been a number of incidents recently in which children were abducted and/or lured to meet adults over these services. Because of these incidents, Congress began exploring ways to limit children's access to these sites, or at least to limit the ability of adults to contact children. During the 109th Congress, H.R. 5319, the Deleting Online Predators Act of 2006 (DOPA), would have amended the Communications Act of 1934 to prohibit schools and libraries receiving "E-Rate" funding from providing access to these types

---

[31] FTC. "Effectiveness and Enforcement of the CAN-SPAM Act: A Report to Congress. " December 2005. See [http://www.ftc.gov/reports/canspam05/051220canspamrpt.pdf].

[32] By Patricia Moloney Figliola, Resources, Science, and Industry Division.

[33] Several laws have been passed related to this issue: Communications Decency Act (CDA) (1996), Child Online Protection Act (COPA) (1998), Children's Internet Protection Act (CIPA) (2000), "Dot Kids" Act (2002), Amber Alert Act (2003), and the Adam Walsh Act (2006).

of websites to minors. The proposal was controversial because the definition of social networking sites could potentially limit access to a wide range of websites, including many with harmless or educational material. Although this bill did not pass, this issue is likely to receive continued attention in the 110th Congress.

"Data retention" is another topic that is likely to receive continued attention from policymakers in the 110th Congress. Data retention is the practice of ISPs maintaining electronic records of subscriber activity, regardless of whether those records have been identified as being needed for an ongoing investigation. At this time, ISPs typically discard records that log subscriber activity when those records are no longer required for business purposes (e.g., network monitoring, billing disputes). However, law enforcement agencies have expressed that they would like data to be retained for longer periods – in general, the time periods suggested have ranged from one to two years – to ensure they can successfully prosecute online child predators and individuals producing and downloading child pornography. Proposals that have been discussed range from simply maintaining records of what websites subscribers visit to requiring the storage of the contents of e-mail messages and individual web pages visited. ISPs have expressed a number of concerns, including the cost of retaining the data, web content being included in data retention legislation, and the privacy and security risks of having such a massive data warehouse available. Opponents of such legislation note that current law already allows law enforcement agencies to mandate data retention for 90-days;[34] further, privacy advocates are concerned that police would potentially be able to obtain records of e-mail chatter, Web browsing, or chat room activity that normally are discarded.

Internet Domain Names[35]

The 110th Congress will continue 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

---

[34] Under 18 USC §2703(f), any governmental entity can require any service provider (telephone company, ISP, cable company, university) to immediately preserve any records in its possession for up to 90 days, renewable indefinitely.

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

Internet and the DNS. Prior to 1993, NSF was responsible for registration of nonmilitary generic Top Level Domains (gTLDs) such as .com, .org, and .net. In 1993, the NSF entered into a five-year cooperative agreement with Network Solutions, Inc. (NSI) to operate Internet domain name registration services. With the cooperative agreement between NSI and NSF due to expire in 1998, the Clinton Administration, through the Department of Commerce (DOC), began exploring ways to transfer administration of the DNS to the private sector.

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

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

Significant disagreements between NSI on the one hand, and ICANN and DOC on the other, arose over how a successful and equitable transition would be made from NSI's previous status as exclusive registrar of .com, org. and net. domain names, to a system that allows multiple and competing registrars. On November 10, 1999, ICANN, NSI, and DOC formally signed an agreement which provided that NSI (now VeriSign) was required to sell its registrar operation by May 10, 2001 in order to retain control of the dot-com registry until 2007. In April 2001, arguing that the registrar business is now highly competitive, VeriSign reached a new agreement with ICANN whereby its registry and registrar businesses would not have to be separated. With DOC approval, ICANN and VeriSign signed the formal agreement on May 25, 2001. On September 17, 2003, ICANN and the Department of Commerce agreed to extend their MOU until September 30, 2006. The MOU specified transition tasks which ICANN has agreed to address, including implementing an objective process for selecting new Top Level Domains; implementing an effective strategy for multi-lingual communications and international outreach; and developing 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.

On June 30, 2005, Michael Gallagher, Assistant Secretary of Commerce for Communications and Information and Administrator of the National Telecommunications and Information Administration (NTIA), stated the U.S. Government's principles on the Internet's domain name system. Specifically, NTIA states that the U.S. Government "intends to preserve the security and stability" of the DNS, and that "the United States is committed to taking no action that would have the potential to adversely impact the effective and efficient operation of the DNS and will therefore maintain its historic role in authorizing changes or modifications to the authoritative root zone file."[36] The NTIA statement also says that governments have legitimate interests in the management of their country code top level domains, that ICANN is the appropriate technical manager of the DNS, and that dialogue related to Internet governance should continue in relevant multiple fora. On May 23, 2006, NTIA announced an inquiry and public meeting seeking comment on the progress of the transition of the technical coordination and management of the DNS to the private sector. The public meeting was held on July 26, 2006.

On September 29, 2006, DOC announced a new Joint Project Agreement with ICANN which continues the transition to the private sector of the coordination of technical functions relating to management of the DNS. The Joint Project Agreement extends through September 30, 2009, and focuses on institutionalizing transparency and accountability mechanisms within ICANN.

Issues

Congressional Committees (primarily the Senate Committee on Commerce, Science and Transportation and the House Committee on Energy and Commerce) maintain oversight on how the Department of Commerce manages and oversees ICANN's activities and policies. Some issues of current concern are discussed below.

Governance. The United Nations (UN), 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 in particular. The study was conducted by the UN's Working Group on Internet Governance (WGIG). On July 14, 2005, the WGIG released its report, stating that no single government should have a preeminent role in relation to international Internet governance, calling for further internationalization of Internet governance, and proposing the creation of a new global forum for Internet stakeholders. Four possible models were put forth, including two involving the creation of new Internet governance bodies linked to the UN. Under three of the four models, ICANN would either be supplanted or made accountable to a higher intergovernmental body. The report's conclusions were scheduled to be considered during the second phase of the WSIS to be held in Tunis in November 2005. U.S. officials stated their opposition to transferring control and administration of the domain name system from ICANN to any international body. Similarly, the 109th

---

[36] Gallagher, Michael, Assistant Secretary of Commerce for Communications, Remarks to the Wireless Communications Association, June 30, 2005. Available at [http://www.ntia.doc.gov/ntiahome/domainname/USDNSprinciples_06302005.pdf].

Congress expressed its support for maintaining U.S. control over ICANN. On November 16, 2005, the House unanimously passed H.Con.Res. 268, which expresses the sense of the Congress that the current system for management of the domain name system works, and that "the authoritative root zone server should remain physically located in the United States and the Secretary of Commerce should maintain oversight of ICANN so that ICANN can continue to manage the day-to-day operation of the Internet's domain name and addressing system well, remain responsive to all Internet stakeholders worldwide, and otherwise fulfill its core technical mission." A similar resolution, S.Res. 323, was passed by the Senate on November 18, 2005 and calls on the President to "continue to oppose any effort to transfer control of the Internet to the United Nations or any other international entity."

The European Union (EU) initially supported the U.S. position. However, during September 2005 preparatory meetings, the EU seemingly shifted its support towards an approach which favored an enhanced international role in governing the Internet. Conflict at the WSIS Tunis Summit over control of the domain name system was averted by the announcement, on November 15, 2005, of an Internet governance agreement between the U.S., the EU, and over 100 other nations. Under this agreement, ICANN and the U.S. will remain in control of the domain name system. A new international group under the auspices of the UN will be formed — the Internet Governance Forum — which will provide an ongoing forum for all stakeholders (both governments and nongovernmental groups) to discuss and debate Internet policy issues. The Internet Governance Forum is slated to run for five years and will not have binding authority. The group held its first meeting on October 30-November 2, 2006 in Athens, Greece. The issue of ICANN and international DNS governance was not formally addressed by the conference.

ICANN-Verisign Agreement and the .com registry. As part of a legal settlement of a long-running dispute between ICANN and Verisign, on February 28, 2006, the ICANN Board of Directors approved (by a vote of 9-5) a new .com registry agreement with Verisign. Under this settlement, Verisign will run the .com registry until 2012 (with a presumption that the agreement will be renewed beyond that date), and will be able to raise domain registration fees by 7% in four of the next six years. These registration fees refer to the current $6 fee that a registrar (such as GoDaddy or Register.com) pays the .com registry operator (Verisign) for each .com domain name registration purchased by the consumer. Under the agreement, Verisign will pay ICANN a one-time sum of $625,000 to implement the agreement, as well as a yearly registry fee, starting at $6 million per year, and going up over the next two years to approximately $12 million.

Critics of the ICANN-Verisign settlement assert that the agreement is anticompetitive, giving Verisign a virtually permanent monopoly over the lucrative .com registry, while also enabling Verisign to raise registration fees without justification. Defenders of the settlement argue that the agreement is necessary to ensure the stability and security of the Internet by ensuring the financial stability of ICANN, and by allowing Verisign the flexibility to raise revenue for upgrading its infrastructure. On June 7, 2006, the House Small Business Committee held a hearing on the ICANN-Verisign .com agreement entitled, "Contracting the Internet: Does ICANN create a barrier to small business?"

The ICANN-Verisign .com agreement was approved by NTIA/DOC on November 30, 2006. As a condition of its approval, NTIA retains oversight over any changes to the pricing provisions of, or renewals of, the new .com registry agreement. Approval of any renewal will occur if NTIA concludes that the approval will serve the public interest in the continued security and stability of the DNS, and in the operation of the .com registry at reasonable prices, terms and conditions.

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

In the 108th Congress, P.L. 108-21/S. 151 (PROTECT Act) contains a provision (Section 108: Misleading Domain Names on the Internet) which 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. In the 109th Congress, the Adam Walsh Child Protection and Safety Act of 2006 (P.L. 109-248), signed into law on July 27, 2006, increases the maximum sentence from four years to ten years for deceiving minors into viewing harmful material.

Meanwhile, on June 1, 2005, ICANN announced that it had entered into commercial and technical negotiations with a registry company (ICM Registry) to operate a new ".xxx" domain, which would be designated for use by adult websites. Registration by adult websites into the .xxx domain would be purely voluntary, and those sites would not be required to give up their existing sites. Announcement of a .xxx domain has proven controversial. With the ICANN Board scheduled to consider final approval of the .xxx domain on August 16, 2005, the Department of Commerce sent a letter to ICANN requesting that adequate additional time be provided to allow ICANN to address the objections of individuals expressing concerns about the impact of pornography on families and children and opposing the creation of a new top level domain devoted to adult content. ICANN's Government Advisory Committee (GAC) also requested more time before the final decision. At the March 2006 Board meeting in New Zealand, the ICANN Board authorized ICANN staff to continue negotiations with ICM Registry to address concerns raised by the DOC and the GAC. However, on May 10, 2006, the Board voted voted 9-5 against accepting the proposed agreement, but did not rule out accepting a revised agreement. Subsequently, on January 5, 2007, ICANN published for public comment a proposed revised agreement with ICM Registry to establish a .xxx domain. The revised agreement would include additional safeguards intended to protect children online.[37]

---

[37] For more information, see:
[http://www.icann.org/announcements/announcement-05jan07.htm]

Meanwhile in the 109th Congress, on March 16, 2006, Senator Baucus introduced the Cyber Safety for Kids Act of 2006 (S. 2426), which would require NTIA to compel ICANN to establish a new top level domain name — such as .xxx — exclusively for material harmful to minors. Websites with material harmful to minors would be required to switch to the new domain. Those that do not would face civil penalties from NTIA.[38] S. 2426 was ultimately not enacted by the 109th Congress.

Trademark Disputes. The increase in conflicts over property rights to certain trademarked names has resulted in a number of lawsuits. The White Paper called upon the World Intellectual Property Organization (WIPO) to develop a set of recommendations for trademark/domain name dispute resolutions, and to submit those recommendations to ICANN. At ICANN's August 1999 meeting in Santiago, the board of directors adopted a dispute resolution policy to be applied uniformly by all ICANN-accredited registrars. Under this policy, registrars receiving complaints will take no action until receiving instructions from the domain-name holder or an order of a court or arbitrator. An exception is made for "abusive registrations" (i.e., cybersquatting and cyberpiracy), whereby a special administrative procedure (conducted largely online by a neutral panel, lasting 45 days or less, and costing about $1000) will resolve the dispute. Implementation of ICANN's Domain Name Dispute Resolution Policy commenced on December 9, 1999. Meanwhile, the 106th Congress passed the Anticybersquatting Consumer Protection Act (incorporated into P.L. 106-113, the FY2000 Consolidated Appropriations Act). The act gives courts the authority to order the forfeiture, cancellation, and/or transfer of domain names registered in "bad faith" that are identical or similar to trademarks, and provides for statutory civil damages of at least $1,000, but not more than $100,000, per domain name identifier.

Privacy. Any person or 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). The scope and accessibility of WHOIS database information has been an issue of contention. Privacy advocates have argued that access to such information should be limited, while many businesses, intellectual property interests, law enforcement agencies, and the U.S. Government have argued that complete and accurate WHOIS information should continue to be publicly accessible. Over the past several years, ICANN has debated this issue through its Generic Names Supporting Organization (GNSO). The GNSO — composed of stakeholder constituencies — is developing policy recommendations on what data should be publicly available through the WHOIS database.

On April 12, 2006, the GNSO approved an official "working definition" for the purpose of the public display of WHOIS information. The GNSO supported a narrow technical definition favored by privacy advocates, registries, registrars, and non-commercial user constituencies, rather then a more expansive definition favored by intellectual property interests, business constituencies, Internet service providers, law enforcement agencies, and the Department of Commerce (through its

---

[38] See CRS Report RL33224, *Constitutionality of Requiring Sexually Explicit Material on the Internet to be Under a Separate Domain Name*, by Henry Cohen.

participation in ICANN's Governmental Advisory Committee). At ICANN's June 2006 meeting, opponents of limiting access to WHOIS data continued urging ICANN to reconsider the working definition. The GNSO will next decide what data should be available for public access in the context of the working definition.[39] On July 18, 2006, the House Committee on Financial Services, Subcommittee on Financial Institutions and Consumer Credit held a hearing on ICANN and the WHOIS database.

Meanwhile, over the past several years, with the WHOIS database continuing to be publically accessible, 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, during the 108th Congress, the Fraudulent Online Identity Sanctions Act was incorporated as Title II of H.R. 3632, the Intellectual Property Protection and Courts Amendments Act of 2004, signed by the President on December 23, 2004 (P.L. 108-482). The act increases criminal penalties for those who submit false contact information when registering a domain name that is subsequently used to commit a crime or engage in copyright or trademark infringement.

Government Information Technology Management[40]

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, some of the most significant information technology management challenges facing the federal government include FCC regulation of converging technologies, funding for information technology research and development, ongoing development and oversight of electronic government (e-government) initiatives, and the growing use of open source software by federal agencies.

---

[39] See ICANN "Whois Services" page, available at [http://www.icann.org/topics/whois-services/]

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

The Federal Communications Commission[41]

One of the most significant issues facing the FCC is the evolution of the communications industry towards an all-digital, broadband world that has blurred the distinctions between services, also called "convergence." The FCC has restructured over the past few years to better reflect the realities of convergence, but the agency is still required to adhere to the statutory requirements of its governing legislation, the Communications Act of 1934. Thus, while convergence has made distinguishing among types of data increasingly difficult, the FCC must continue to differentiate among services based on the distinctions drawn in the 1934 Act. Unfortunately, when all data looks 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 begin to appear more strained.

The FCC has continued to address a number of issues directly related to convergence: the regulatory classification of services via the Internet protocol (e.g., voice over Internet Protocol [VoIP]) and law enforcement's ability to conduct wiretaps effectively (i.e., using the Communications Assistance for Law Enforcement Act [CALEA]). During the 110th Congress, as there was during the 109th Congress, there may be legislation to enact a national franchising system for video service providers. If so, this will likely require additional attention from the FCC as well.

The FCC will also remain focused on broadband deployment. The agency will continue to monitor its policies to encourage new providers to roll out new services (e.g., power companies will be deploying broadband over powerlines [BPL]) as well as continue to promote deployment to underserved areas and populations, i.e., 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 now intersect. So many of the broadband issues are inter-related that it is often difficult to sort out where one issue ends and another begins. For example, VoIP, CALEA, and BPL are all tied to the concept of broadband convergence and reliance on the Internet for information and 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 both the FCC and Congress in the near future.

---

[41] 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*, by Patricia Moloney Figliola; and CRS Report RL33542, *Broadband Internet Access: Background and* Issues by Angele A. Gilroy and Lennard G. Kruger, both of which are updated more frequently than this report.

Information Technology R&D[42]

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. The FY2007 budget calls for $3.074 billion for the NITRD Program, an increase of $0.21 billion over the FY2006 budget estimate of $2.855 billion.

Research emphases are focused on eight program component areas (also called PCAs): High-End Computing (HEC) Infrastructure and Applications, HEC Research and Development, Cyber Security and Information Assurance, Human Computer Interaction and Information Management, Large Scale Networking, Software Design and Productivity, High Confidence Software and Systems, and Social, Economic, and Workforce Implications of IT and IT Workforce Development. Key issues facing congressional policymakers include whether NITRD is accomplishing its goals and objectives to enhance U.S. information technology research and development, whether the funding level is appropriate or should be changed to reflect changing U.S. priorities, and defining the private sector's role in this initiative.

Electronic Government (E-Government)[43]

Electronic government (e-government) is an evolving concept, meaning different things to different people. However, it has significant relevance to four important areas of governance: (1) delivery of services (government-to-citizen, or G2C); (2) providing information (also G2C); (3) facilitating the procurement of goods and services (government-to-business, or G2B, and business-to-government, or B2G); and (4) facilitating efficient exchanges within and between agencies (government-to-government, or G2G). For policymakers concerned about e-government, a central area of concern is developing a comprehensive but flexible strategy to coordinate the disparate e-government initiatives across the federal government.

---

[42] By Patricia Moloney Figliola, Resources, Science, and Industry Division. See also CRS Report RL33586, *The Federal Networking and Information Technology Research and Development Program: Funding Issues and Activities*, by Patricia Moloney Figliola, which is updated more frequently than this report.

[43] 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*, by Jeffrey W. Seifert, which is updated more frequently than this report.

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], which first went online on September 22, 2000. 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.[44] 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 four categories; government-to-citizen, government-to-government, government-to-business, and internal effectiveness and efficiency. Examples of these initiatives include an e-authentication project led by the General Services Administration (GSA) to increase the use of digital signatures, the eligibility assistance online project (also referred to as GovBenefits.gov) led by the Department of Labor to create a common access point for information regarding government benefits available to citizens, and the Small Business Administration's One-Stop Business Compliance project, being designed to help businesses navigate legal and regulatory requirements. A 24th initiative, a government wide payroll process project, was subsequently added by the President's Management Council. In 2002 the e-Clearance initiative, originally included as part of the Enterprise Human Resources Integration project, was established as a separate project, for a total of 25 initiatives. Since that time, the Bush Administration has reclassified the e-Authentication

---

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

initiative as "a separate initiative that provides secure and robust authentication services to the 24 [i]nitiatives," bringing the official tally again to 24 initiatives.[45]

As the initial round of e-government projects has matured, OMB has focused attention on initiatives that consolidate information technology systems in nine functional areas, or Lines of Business (LoB). These include financial management, human resource management, grants management, case management, federal health architecture, information security, budget formulation and evaluation, geospatial systems, and information technology infrastructure. These initiatives were chosen, in part, because they represent core business functions common to many departments and agencies, and/or have the potential to reap significant efficiency and efficacy gains. These LoB initiatives are anticipated to create $5 billion in savings over 10 years.

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 110th Congress, continued oversight of the Quicksilver projects, the implementation of the E-Government Act, and the development and funding of the second generation Lines of Business e-government initiatives are the primary oversight 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.whitehouse.gov/omb/egov/a-1-fea.html]; 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[46]

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. A growing number of state and local governments have also been exploring the official adoption of open source software. Likewise, open source software may also play a role in the growth of regional health information organizations (RHIOs), as part of an effort to spread the use of e-health records. 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,

---

[45] See [http://www.whitehouse.gov/omb/egov/c-presidential.html].

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

improving government information technology management practices, strengthening computer security, and protecting intellectual property rights. In the 110th Congress, the debate over open source software is anticipated to revolve primarily around information security and intellectual property rights, including the possible development of a legal definition of open source software. However, issues related to cost and quality are likely to be raised as well.

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

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 official U.S. federal government policy regarding the use of open source software by government agencies is described in a July 2004 Office of Management and Budget (OMB) memorandum on software acquisition, M-04-16 Memoranda for Senior Procurement Executives, Chief Information Officers, *Software Acquisition*. The memorandum states that the policies guiding government information technology investment decisions are "technology and vendor neutral" and that agencies' technology choices "must be consistent with the agency's enterprise architecture and the Federal Enterprise Architecture."[47] Agencies are also instructed to take into account a number of other merit-based factors, including information security, licensing requirements, and total cost of ownership. Implicit in these

---

[47] For more information about enterprise architectures generally, and the Federal Enterprise Architecture (FEA) specifically, see CRS Report RL33417, *Federal Enterprise Architecture and E-Government: Issues for Information Technology Management*, by Jeffrey W. Seifert.

requirements is an expectation that agencies will also make choices based on the quality of the product.

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

Appendix A: List of Acronyms

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 B: Legislation Passed by the 105th-109th 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.

The **Deficit Reduction Act of 2005 (P.L. 109-171)**, Title III sets a hard deadline for the digital television transition, thereby reclaiming analog television spectrum to be auctioned for commercial applications such as wireless broadband.

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.

The **Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2005 (US SAFE WEB), P.L. 109-455** would allow the Federal Trade Commission and parallel foreign law enforcement agencies to share information while investigating allegations of "unfair and deceptive practices" that involve foreign commerce.

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, *Internet: Status Report on Legislative Attempts to Protect Children from Unsuitable Material on the Web*, by Patricia Moloney Figliola, 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.

The **Adam Walsh Child Protection and Safety Act of 2006 (P.L. 109-248)** increases the penalty from 4 to 10 years imprisonment for persons who knowingly use a misleading domain name with the intent to deceive a minor into viewing harmful material.

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, *Obscenity, Child Pornography, and Indecency: Recent Developments and Pending Issues*, by Henry Cohen, 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.

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

Table 5. Summary of Legislation Passed by the 109th Congress

Title	Public law number
Deficit Reduction Act of 2005 (Title III, Digital Television Transition and Public Safety)	P.L. 109-171
Adam Walsh Child Protection and Safety Act of 2006	P.L. 109-248
Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2005 (US SAFE WEB)	P.L. 109-455