98-67 STM

CRS Report for Congress

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

Updated August 25, 2000

Marcia S. Smith, Richard M. Nunno,
John D. Moteff, and Lennard G. Kruger
Resources, Science, and Industry Division

Congressional Research Service • The Library of Congress

The Congressional Research Service works exclusively for the Congress, conducting research, analyzing legislation, and providing information at the request of committees, Members, and their staffs.

The Service makes such research available, without partisan bias, in many forms including studies, reports, compilations, digests, and background briefings. Upon request, CRS assists committees in analyzing legislative proposals and issues, and in assessing the possible effects of these proposals and their alternatives. The Service's senior specialists and subject analysts are also available for personal consultations in their respective fields of expertise.

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

Summary

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

1. The long-running **encryption** debate concerns balancing the interests of personal privacy, competitiveness of U.S. computer companies, and law enforcement and national security requirements in setting limits on what encryption products can be exported.

2. **Electronic signatures** are of congressional interest both in terms of the respective roles of federal versus state laws governing their use and requiring government use of electronic signatures to enable electronic filing of information.

3. Concerns about **computer security**, particularly unauthorized access or "hacking," are prevalent both in government and the private sector. Issues also have been raised about the vulnerability of the nation's critical infrastructure (e.g., electrical power grids and telecommunications) to cyber attacks.

4. Individuals and businesses considering whether to use the Internet are increasingly concerned about **Internet privacy**, particularly of personally identifiable information. While Congress and the Administration both hope industry self-regulation will solve these problems, a law protecting children's privacy was passed last year and several bills are pending in the 106th Congress.

5. **Protecting children from unsuitable material** on the World Wide Web has been a major focus of concern. A law passed by the 105th Congress (the Child Online Protection Act) is currently being challenged in the courts. Congress is also debating whether certain schools and libraries should be required to use filtering technology.

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

7. The administration and governance of the **Internet's domain name system** (DNS) is currently under transition. Issues for the 106th Congress include how domain name trademark disputes will be resolved, and the progress of the federal government's efforts to transfer control of the DNS to the private sector.

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

Contents

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

The continued growth of the Internet for personal, government, and business purposes may be affected by a number of issues being debated by Congress. Among them are establishing "trustworthiness" by authenticating and verifying the origin and content of messages, safeguarding system security, ensuring the privacy of information collected by Web site operators, protecting children from unsuitable material, limiting unsolicited commercial electronic mail, the administration and governance of the Internet domain name system, and access to broadband services. This report provides short overviews of each of these issues from a technology policy perspective, referencing other CRS reports for more detail. Related legislation is identified and a list of the bills introduced in the 106th Congress by topic is provided at the end.

Summary of Legislation Passed by the 105th Congress

The 105th Congress considered a wide variety of bills related to Internet issues, but only a few finally passed both chambers and were sent to the President. Of the issues covered in this report, legislation was enacted concerning protecting children, identity theft, intellectual property, digital signatures, and Internet domain names. (Legislation concerning Internet taxes also passed. That topic per se is not included in this report. See: *Internet Tax Bills in the 105th Congress*, CRS Report 98-509 E, by Nonna Noto. However, the Act also included language relating to protecting children, so is discussed in that context).[1]

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

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

---

[1]Internet gambling also was debated the 105th Congress and continues to be controversial in the 106th. That issue is not addressed in this report. See CRS Report RS20485, *Internet Gambling: A Sketch of Legislative Proposals*, by Charles Doyle.

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

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

The Omnibus Appropriation Act also includes a provision intended to make it easier for the FBI to gain access to Internet service provider records of suspected sexual predators (Section 102, General Provisions, Justice Department). It also sets aside $2.4 million for the Customs Service to double the staffing and resources for the child pornography cyber-smuggling initiative and provides $1 million in the Violent Crime Reduction Trust Fund for technology support for that initiative.

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

Identity Theft and Assumption Deterrence Act

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

Intellectual Property: Digital Millennium Copyright Act

Congress passed legislation (P.L. 105-304) implementing the World Intellectual Property Organization (WIPO) treaties regarding protection of copyright on the Internet. The law also limits copyright infringement liability for online service providers that serve only as conduits of information. Provisions relating to database protection that were included by the House were not included in the enacted version

and are being debated anew in the 106th Congress. Since database protection per se is not an Internet issue, it is not included in this report (see CRS Report 98-902, *Intellectual Property Protection for Noncreative Databases*).

Digital Signatures: Government Paperwork Elimination Act

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

Internet Domain Names: Next Generation Internet Research Act

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

Table 1. Related Legislation Passed by the 105th Congress

Title	Public Law and Bill Numbers
FY1999 Omnibus Consolidated and Emergency Supplemental Appropriations Act	**P.L. 105-277 H.R. 4328**
Division C, Title XI: Internet Tax Freedom Act	H.R. 1054/S. 442
Division C, Title XIII: Children's Online Privacy Protection Act	S. 2326
Division C, Title XIV: Child Online Protection Act	H.R. 3783/S. 1482
Division C, Title XVII: Government Paperwork Elimination Act	S. 2107
Protection of Children from Sexual Predators Act	**P.L. 105-314 H.R. 3494/S. 2491**
Identity Theft and Assumption Deterrence Act	**P.L. 105-318 H.R. 4151/S. 512**
Digital Millennium Copyright Act	**P.L. 105-304 H.R. 2281/S. 2037**
Next Generation Internet Research Act	**P.L. 105-305 H.R. 3332/S. 1609**

Encryption[2]

Encryption and decryption are methods of applying the science of cryptography to ensure the privacy of data and communications. The long-running encryption debate concerns balancing the interests of personal privacy, competitiveness of U.S. computer companies, and law enforcement and national security requirements.

Cryptography traditionally has been the province of those seeking to protect military secrets, and until the 1970s relied on "secret key" cryptography where the sender and the recipient both had to have the same key. Thus a trusted courier or some other method was required to get the key from the sender to the recipient. The advent of "public key cryptography" in 1976 made it possible for encryption to be used on a much broader scale. In this form of cryptography, each user has a pair of keys: a public key available to anyone with which a message can be encrypted, and a private key known only to that user with which messages are decrypted. The "key pair" is electronically generated by whatever encryption product is used. In a hypothetical example, if Bob wants to sent a private e-mail message to Carol and ensure that no one else can read it, he obtains Carol's public key from Carol herself or from a publicly available list. Using Carol's public key, Bob encrypts his message. When Carol receives the message, she uses her private key to decrypt it. To reply to Bob, Carol gets Bob's public key from Bob or from a publicly available list and uses it to encrypt her response. When Bob receives the message, he uses his private key to decrypt it.

Use of strong (difficult to break) encryption is considered vital to the growth in use of the Internet, particularly for electronic commerce, because businesses and consumers want to protect the privacy of information exchanged via computer networks. When a message is encrypted, it is referred to as "ciphertext." That message is called "plaintext" before it is encrypted and after it has been decrypted. The Clinton Administration wants to ensure that authorized law enforcement officials and government entities can access the plaintext of a message if undesirable activity is suspected (terrorism, drug trafficking, and child pornography are often cited as examples). If the message is encrypted, they either have to break the encryption by "brute force" (trying all possible combinations until they get the right one), or get access to the decryption key.

Export Restrictions and Domestic Use

The congressional debate over U.S. encryption policy has evolved from a time when the competing interests diverged widely concerning individual rights to privacy, the global competitiveness of U.S. companies selling encryption products, the promotion of secure electronic commerce, and law enforcement and national security needs to monitor undesirable behavior. The Clinton Administration originally supported the wide use of strong encryption as long as it had a feature called "key recovery" to allow authorized law enforcement agents to access the plaintext in a timely manner by getting access to the decryption key. This raised privacy issues. The

---

[2] See also CRS Issue Brief IB96039, *Encryption Technology: Congressional Issues*, which is updated more frequently than this report.

Administration also sought to influence what type of products are available domestically by limiting exports, knowing that companies would not sell strong encryption products domestically and weak ones for export. This raised industry concerns about placing U.S. computer hardware and software companies at a competitive disadvantage because they were subject to export restraints.

In December 1996, the Clinton Administration released temporary (two-year) export regulations designed to encourage computer hardware and software manufacturers to develop and implement key recovery technologies. Although there are other factors that affect the strength of an encryption product, the number of binary digits (bits) in the key has been used as the benchmark in this debate. The larger the number of bits, the more difficult it is to break the encryption. Under the interim regulations, companies were allowed to export 56 bit encryption products if they agreed to incorporate key recovery features into the product within the two years. If they already incorporated key recovery into the product, there was no limit on the bit length that could be exported (with some exceptions for banking.) Previously, only 40 bit encryption could be legally exported.

In September 1998, the Clinton Administration announced plans to permanently reduce its restrictions on the use and export of encryption. The policy allowed the export of 56-bit encryption products without requiring provisions for key recovery, after a one-time review, to all users outside of seven "terrorist countries." The policy applied only to U.S. companies in the finance, health care, insurance, and electronic commerce industries. Export of encryption products of any strength was permitted to 42 designated countries if key recovery or access to plaintext was provided to an approved third party. The Administration also supported the FBI's technical support center to help law enforcement in keeping abreast of encryption technologies.

On September 16, 1999, the Administration again announced changes to its encryption policy, making encryption products of any key length, after a technical review, exportable without a license to users in any country except seven "terrorist countries". Exporters must report to the government on where the encryption product is exported, reflecting industry business models and distribution channels. In addition, the President proposed legislation that would ensure that law enforcement agencies maintain their ability to access decryption information stored with third parties, and allow information on techniques used in decryption to be withheld in court. The bill would also authorize $80 million over four years for the FBI Technical Support Center, which will serve as a technical resource in responding to the use of encryption by criminals. To date, no Member has introduced that legislation. (Other pending legislation is discussed below.)

The regulations implementing the Administration's new encryption export policy were issued by the Department of Commerce's Bureau of Export Administration (BXA) on January 14, 2000. According to the rules, retail encryption commodities and software of any key length can be exported without a license to any non-government end user in any country except the seven state supporters of terrorism, and can be re-exported to anyone (including Internet and telecommunications service providers). Exports previously allowed only for a company's internal use can now be used for communication with other firms, supply chains, and customers. Exports to most government end-users still require a license, but, on July 17, 2000, the

Administration updated its policy to enable exports without a license to European Union and certain other governments. Exporters must report to BXA where the encryption product is exported, and BXA will determine whether products qualify as retail by reviewing their functionality, sales volume, and distribution methods. The Administration accepted public comments on the feasibility of the regulation for 120 days, and a final rule is pending.

While the computer industry is satisfied with these rules, some privacy rights groups argue that there are still ambiguities in the rules, and the rules make encryption technology overly cumbersome for individuals to use. Because the regulations could be reversed by a future Administration, some still advocate the passage of legislation to codify the changes in U.S. encryption policy. Based on the decrease in congressional activity on the issue, the latest rules may have struck a balance among competing interests regarding U.S. encryption policy.

Key Recovery

The term "key recovery" (formerly called key escrow) refers to a system whereby a party external to the user holds a copy of the decryption key. (Other mechanisms could also be employed to achieve the same result—e.g., the key could be split among two or more key recovery agents for added security). Having access to such a "spare key" through a key recovery agent could be desirable for a user if a key is lost, stolen, or corrupted. Most parties to the encryption debate agree that market forces will drive the development of key recovery-based encryption products for stored computer data because businesses and individuals will want to be sure they can get copies of keys in an emergency. The debate is on the role of the government in "encouraging" the development of key recovery-based encryption, whether key recovery agents should be required to provide keys to duly authorized law enforcement officials, and the government's role in determining who can serve as key recovery agents. Since 1998, key recovery business plans are no longer required, and the regulatory requirements for key recovery agents have been reduced.

Another element needed for the widespread use of encryption is certificate authorities to issue and manage electronic certificates (electronic records that identify a user within a secure information system) and verify that a particular individual is associated with a particular public key. This is especially important for the conduct of electronic commerce, for example, where buyers and sellers want to be assured of each other's identities. Privacy rights advocates argue that the ability to issue certificates should be independent from the debate over key recovery, making controversial any linkage between certificate authorities and key recovery. The combination of public key encryption and certificate authorities (some would add key recovery agents) is referred to as a "public key infrastructure" (PKI). The establishment of one or more PKIs globally is expected to add the requisite element of "trust" to the Internet needed for its use to expand. H.R. 2413 (Sensenbrenner), introduced July 1, 1999, calls for a National Research Council study of PKIs.

The Clinton Administration has not changed its policy that allows any type of encryption to be sold in or imported into the United States. However, on September 3, 1997, FBI Director Louis Freeh discussed domestic use restrictions at a hearing before the Senate Judiciary Committee's Subcommittee on Technology, Terrorism

and Government Information. He expressed the point of view that only encryption products with key recovery be sold or imported for sale in the United States. Apparently the FBI also had drafted legislation along those lines (reportedly for a House committee) and the issue of domestic use restraints has become an integral part of the encryption debate. The Administration never proposed domestic use restraints, but it did not prevent the FBI Director from promoting that course of action. Civil liberties groups in particular are opposed to domestic use controls.

105th Congress

There were seven bills in the 105th Congress addressing these encryption issues, none of which was enacted. Six of the bills addressed the export issue: H.R. 695 (Goodlatte, as introduced), S. 376 (Leahy), S. 377 (Burns), and S. 909 (McCain) sought to relax export controls on encryption, although versions of H.R. 695 as reported from various committees had substantially different provisions. (S. 909 provided that the 56 bit limit could increase as recommended by an Encryption Export Advisory Board established by the Act unless the President determined it would harm national security, and allowed the President to waive any provision, including the export limits, in the interest of national security, or domestic safety and security.) S. 2067 (Ashcroft) allowed the removal of controls for encryption products generally available in the international market, and allowed the Department of Justice to create a National Electronic Technologies Center to assist law enforcement in gaining efficient access to plaintext of communications and electronic information. The section of H.R. 1903 (Sensenbrenner) that dealt with export issues was deleted before it passed the House, but the bill still called for export policy to be determined in light of the "public availability of comparable technology."

106th Congress

Divisions remain between those who oppose a liberal encryption policy (national security and law enforcement officials) and those who advocate it (computer industry representatives and privacy rights advocates). The Security and Freedom Through Encryption Act (H.R. 850, Goodlatte), introduced February 25, 1999 (similar to H.R. 695 from the 105th Congress), would foster the widespread use of the strongest encryption, with additional provisions to create criminal penalties for the use of encryption to conceal criminal conduct, and direct the Attorney General to compile examples in which encryption has interfered with law enforcement. The bill was reported (without amendment) by the Judiciary Committee on April 27 (H.Rept.106-117 part I), and was referred jointly and sequentially to the Committees on International Relations, Commerce, Armed Services, and Permanent Select on Intelligence. The bill was reported (amended) by the each of the other four Committees (Parts II, III, IV, and V).

The five versions of H.R. 850 differ significantly, and provisions written into some versions completely oppose other versions. The versions passed by the Committees on the Judiciary, Commerce, and International Relations codify the policy of unrestricted domestic use and sale of encryption, prohibit the government from mandating key escrow practices for the public, and liberalize the controls governing the export of strong encryption. The Armed Services and Intelligence Committee

versions, in contrast, have minimal or no mention of domestic use of encryption, and increase the authority of the President in restricting the controls governing the export of strong encryption. All of the bills, except for the version by the Armed Services Committee, establish criminal penalties for the use of encryption in the furtherance of a criminal act. The Intelligence Committee version, however, provides greater details than the others for criminalizing the use of encryption in a criminal act.

In addition, each Committee added provisions for specific agencies and circumstances. For example, the Commerce Committee established a National Electronic Technologies (NET) Center in the Department of Commerce to promote the exchange of information regarding data security techniques and technologies, and the International Relations Committee directed the Secretary of Commerce to consult with the Attorney General, the Federal Bureau of Investigation, and the Drug Enforcement Administration before approving any license to export encryption products to any country identified as being a major drug producer. The Intelligence Committee authorizes appropriations for the Technical Support Center, at the FBI.

In the Senate, S. 798 (McCain) was introduced on April 14, 1999, containing similar provisions as the original version of H.R. 850, except that it only allows the export of encryption products with 64 bit key lengths or less, and establishes an Encryption Export Advisory Board that could recommend allowing the export of stronger products in the future. S. 798 also sets a deadline of January 1, 2002 for the federal adoption of the Advanced Encryption Standard (which uses a 128 bit key length) and allows the export of products employing AES at that date. S. 798 allows the export of strong (greater than 64 bit) encryption products with key recovery features, as well as the export of strong encryption products to "legitimate and responsible entities," including publicly traded firms, U.S. corporate subsidiaries or affiliates, firms required by law to maintain plaintext records, and others. S. 798 does not contain criminal provisions for the use of encryption in the furtherance of a crime (unlike H.R. 850), and prohibits domestic controls and mandatory plaintext access.

While some elements of this legislation might be resolved in conference, reaching a compromise on some of the differences (such as key escrow and export policies) may be difficult. The prospects for enacting legislation are further complicated by the possible veto by President Clinton if the final bill passed by Congress is not supported by officials in the Defense and Justice Departments. On July 27, two more encryption policy-related bills were introduced: H.R. 2616 (Goss), which reflects the House Intelligence Committee's mark-up of H.R. 850, and H.R. 2617 (Goss), which proposes a tax incentive for the nation's encryption software manufacturers to develop products with recoverability features. After the Administration's relaxation of encryption regulations, the pressure dissipated to bring H.R. 850 to the floor in the House.

Electronic Signatures/Digital Signatures

An electronic signature is a means of uniquely identifying (*authenticating*) the user of a computer to control access or authorize a transaction. Electronic signatures can use several technologies including personal identification numbers, smart cards, biometrics (i.e., digital fingerprints, retinal scans, or voice recognition), or digital signatures (an encrypted set of bits that identify the user). Electronic signatures can be used for access or control of either stand-alone computers or of Internet-based transactions. The most common electronic signature technology in use today is the digital signature, which is unique to each individual and to each message, and can be used in conjunction with certificate authorities to verify that the individuals on each end of a communication are who they claim to be and to authenticate that nothing in the message has been changed. Through the use of digital signatures, legally recognized signatures can be produced for use in electronic commerce. A digital signature is distinguished from an encryption product in that a digital signature does not provide *confidentiality* (preventing transmitted data from being monitored by unwanted parties).

Electronic signatures are of congressional interest both in terms of the respective roles of federal, state, and international laws governing their use and requirements for government use of electronic signatures to enable electronic filing of information. While neither law enforcement nor national security organizations oppose the use of electronic signatures, many question whether a standard for electronic signatures should be established to enhance electronic commerce. With the exception of Arkansas, South Carolina, and South Dakota, all states have considered or enacted some form of electronic authentication law. Thirty-six states have introduced or are considering 76 electronic signature initiatives. Twenty-six states have enacted one or more of these initiatives into law. In the area of digital signatures or PKI technologies, 20 states have introduced or considered 36 different initiatives or regulations with 10 states adopting some form into law. Seven states are examining laws that address both digital and electronic signatures. These laws are summarized in *Survey of State Electronic & Digital Signature Legislative Initiatives* by Albert Gidari and John Morgan of Perkins Cole. The article, and links to state laws, are provided by the Internet Law and Policy Forum [http://www.ilpf.org/digsig/UPDATE.htm].

According to Gidari and Morgan, three models have developed at the state level: the "Utah" or "prescriptive" model with a specific public key infrastructure scheme including state-licensed certificate authorities; the "California" or "criteria-based" model that requires digital or electronic signatures to satisfy certain criteria of reliability and security; and the "Massachusetts" or "signature enabling" model that adopts no specific technological approach or criteria, but recognizes electronic signatures and documents in a manner parallel to traditional signatures. Some of the proposed state laws are general, applying to a wide range of government or private sector activities, while others are more narrowly cast. One controversial aspect of the debate over electronic and digital signatures is whether there should be a single federal law in place of the various state laws.

Enacted Laws from Previous Congresses

In the 105th Congress, the Government Paperwork Elimination Act was enacted as part of the Omnibus Appropriations Act (P.L. 105-277). This measure directs the Office of Management and Budget (OMB) to establish procedures for executive branch agencies to accept electronic submissions using electronic signatures, and requires agencies to accept those electronic submissions except where found to be impractical or inappropriate. By October 2003, executive branch agencies must provide for the option of electronic maintenance, submission, or disclosure of information as a substitute for paper. In April 2000, OMB released procedures to permit private employers to electronically store and file with executive agencies forms pertaining to their employees. In addition, OMB, together with the National Telecommunications and Information Administration, is conducting a study of the use of electronic signatures, including an analysis of its impact on paperwork reduction, electronic commerce, individual privacy, and the security and authenticity of electronic transactions, and will report to Congress on these issues. Electronic records generated from this law will have full legal effect, and information collected from an executive agency using electronic signature services may only be used or disclosed by those using the information for business or government practices. These provisions do not apply to the Department of Treasury if the provisions conflict with internal revenue laws or codes. On March 5, 1999, OMB released proposed procedures to implement the Act, outlining actions for specific federal agencies. Some of those who commented on the OMB proposal were concerned about a potential over-reliance on "identity-based" authentication techniques that could lead to larger storehouses of information collected by the government and its contractors.

Another issue is whether the government should use commercial standards for electronic or digital signatures. Since 1993, the federal government had adopted only the federally developed Digital Signature Algorithm (DSA), which does not support confidentiality. In December 1998, however, after the enactment of the National Technology Transfer Act of 1995 (P.L. 104-113) and with policies established in OMB Circular A-119 (revised February 10, 1998), the National Institute of Standards and Technology (NIST) announced approval of an interim Federal Information Processing Standard (FIPS) to allow federal agencies to use the RSA digital signature standard (the de facto commercial standard) in addition to the DSA standard. Permanent adoption of the RSA standard could increase its use by firms that conduct business with the federal government. NIST is also reviewing a third digital signature standard, called Elliptic Curve Cryptography (ECC), which, if adopted, could result in a more competitive market for digital signature software.

Legislation in the 106th Congress

In the 106th Congress, several bills were been introduced regarding electronic and digital signatures. The Millennium Digital Commerce Act (S. 761, Abraham and its companion H.R. 1320, Eshoo), introduced March 25, 1999, would regulate interstate electronic commerce by permitting and encouraging its continued expansion through the operation of free market forces, including the legal recognition of electronic signatures. S. 761 was referred to the Senate Commerce Committee and was reported by the Committee with an amendment on July 30 (S. Rept. 106-131). The

bill passed the Senate (amended) on November 19. H.R. 1320 was referred to the House Commerce and Government Reform Committees, and no further action was taken on that bill. Another similar (but broader) bill, Electronic Signatures in Global and National Commerce Act (H.R. 1714, Bliley), introduced May 6, 1999, would facilitate the use of electronic signatures and records (i.e., a document created, stored, generated, received, or communicated by electronic means) in interstate and foreign commerce. Two different amended versions of H.R. 1714 were reported by the House Commerce Committee (H. Rept. 106-341 part I, September 27) and the House Judiciary Committee (H. Rept. 106-341 part II, October 15), and the bill passed the House on November 9, 1999.

Businesses generally favored both House and Senate versions of this legislation, but the Administration and some consumer and privacy advocates were concerned that the language in the House bill may be overly broad or undefined, and could create disadvantages for consumers who do not have access to computers or the Internet. Furthermore, the National Conference of Commissioners on Uniform State Laws expressed concern that the legislation could interfere with the efforts of some states to adopt electronic signature laws. The conference report (H. Rept. 106-661) passed the House June 14 and the Senate June 16, and was signed by the President (P.L. 106-229) on June 30.

Other bills with electronic and digital signature provisions include: (1) the Paperwork Elimination Act of 1999 (H.R. 439, Talent), introduced February 2, 1999, is intended to minimize the burden of federal paperwork demands upon small businesses, educational and nonprofit institutions, federal contractors, state and local governments, and other persons through the sponsorship and use of electronic signatures and records, including over the Internet (passed House February 9, 1999, received in the Senate February 11, referred to the Committee on Governmental Affairs February 22); (2) the Digital Signature Act (H.R. 1572, Gordon), introduced April 27, would require the adoption and utilization of digital signatures by federal agencies and establish a national policy panel for digital signatures, with government, academic, and industry representatives, to study the use of digital signatures in private sector electronic transactions, such as over the Internet (referred to the Committee on Science); (3) the Internet Growth and Development Act of 1999 (H.R. 1685, Boucher), introduced May 5, 1999, contains a provision to provide for the recognition of electronic signatures for the conduct of interstate and foreign commerce (referred to Committees on Commerce and Judiciary); (4) Computer Security Enhancement Act of 1999 (H.R. 2413, Sensenbrenner), introduced July 1, 1999, contains a provision directing the National Institute of Standards and Technology to develop electronic authentication (i.e., electronic signature) infrastructure guidelines and standards for use by federal agencies to effectively utilize electronic authentication technologies in a manner that is sufficiently secure and interoperable to meet the needs of those agencies and their transaction partners (referred to Committee on Science; marked-up by Technology Subcommittee October 20); and (5) the Electronic Securities Transactions Act (S. 921, Abraham), introduced April 29, 1999, would facilitate and promote electronic commerce in securities transactions involving broker-dealers, transfer agents and investment advisers (referred to Committee on Banking).

Computer Security

Although unauthorized access to computer networks ("hacking") is by no means a new problem, growing use of the Internet increases the threat and risk. Hacking or "cracking"(hacking with the intent to do harm) is perceived to be a growing problem both for the government and the private sector. The extent of the problem is difficult to quantify because many institutions do not want the negative publicity associated with public acknowledgment of hacking attempts (whether successful or not). Also, many attempts to hack into a computer system may go undetected.

A 1996 report by the Senate Governmental Affairs Permanent Select Subcommittee on Investigations, together with a related series of hearings and a General Accounting Office report (GAO/AIMD-96-84) have provided some estimates. The GAO study referenced an assessment by the Defense Information Systems Agency that Department of Defense computers may have been attacked 250,000 times during 1995. The assessment added that the number may represent just a small fraction of the attempts because only an estimated 1 in 150 attacks are detected and reported. What constitutes an "attack" must be defined, however. Some "attacks" may be someone "pinging" a system to get an idea of how a system is structured or looking for weak access points (like walking down the hall in a hotel and checking the doors to see if they are locked) and may never result in an intrusion per se. Regarding the private sector, the subcommittee's report cited an estimate from one private security company that the private sector had lost $800 million in 1995 due to computer intrusions. Most losses probably are not publicly acknowledged, however.

In its most recent survey (1999) conducted in cooperation with the FBI, the Computer Security Institute (CSI) reported that of the 521 responses from commercial, government, and academic security practitioners, 62% reported security breaches (a slight drop in percentage from the 1998 survey results). Breaches included theft of proprietary information, sabotage, insider abuse of Internet access, financial fraud, spoofing, denial of service, viruses, telecommunications fraud, wiretapping, eavesdropping, and laptop theft.[3] Based on respondents' estimates, total financial losses amounted to $124 million (also down from the 1998 survey results). However, only 31% of those reporting losses were able to quantify them. Therefore, the financial losses may be much greater. Financial losses include not only direct costs (theft of funds, costs to repair databases) but also indirect costs such as system "down-time" and, if measurable, losses due to loss of confidence. Tables from the CSI report and a press release are available at [http://www.gocsi.com/prelea990301.htm].

Computer security administrators lament that not enough attention and resources are being paid to the security risks associated with networked systems. Even where

---

[3]Reports of unauthorized access to credit card numbers stored on computers also have attracted much interest. Not only is there the risk of direct financial loss from someone using a credit card without authorization of the card owner, but increasingly people are concerned about consumer identity theft that involves use of another's personally identifiable information such as credit card numbers. That issue is addressed below.

the problems are recognized, fixes needed to solve "Year 2000" (Y2K) problems (see CRS Issue Brief IB97036) took precedent. Now that the Y2K has passed for the most part, the market for computer security assessments and security products should grow even more. And, because of the demand for knowledgeable personnel, many former "hackers" are making legitimate money in the security business. Some security specialists insist that this is not without its risks.

Rules and regulations governing the security of federal computer systems are guided by the Computer Security Act of 1987 (P.L. 100-235), and OMB Circular A-130, Annex III. The Act requires each agency to develop a security plan for those computer systems containing sensitive information. The plans are to be reviewed by experts within the National Institute of Standards and Technology (NIST) or the National Security Agency (NSA). A summary of the plans are to be forwarded to the Office of Management and Budget (OMB) along with their overall budget plans for information technology. OMB chairs an interagency committee of Chief Information Officers (CIOs) in which a subcommittee is devoted to security issues. In addition, the Act authorizes the National Institute of Standards and Technology (NIST) to set security standards for all civilian unclassified government systems. The National Security Agency (NSA) does the same for the federal government's classified computer systems. NIST and NSA have formed a partnership, along with a few other foreign countries, that is providing common criteria for certifying security products. This partnership facilitates an international market in security products.

Various federal agencies also have groups that will perform vulnerability analyses on federal systems, recommend fixes to problems identified, and to assist in integrating those fixes into systems. A variety of agencies have also set up computer emergency response teams (CERTs) that help system administrators deal with intrusions and the problems that might arise. The CERT at Carnegie Mellon University was established to provide such services to Internet users anywhere in the country and has signed a contract with the General Services Administration to provide similar services to government agencies that may not have their own capability.

Of growing concern is the risk hacking poses to America's basic infrastructures (e.g., transportation systems, electric utilities), which increasingly rely on networked computer systems. The President's Commission on Critical Infrastructure Protection (PCCIP) issued a report in November 1997 regarding the "cyberthreat" to five of the nation's basic infrastructures—information and communications, banking and finance, energy (including electric power, oil, and gas), physical distribution, and vital human services. While not finding an immediate crisis, the PCCIP concluded that the nation's infrastructures are vulnerable and the consequences threatening to the security of the nation. The report, *Critical Foundations: Protecting America's Infrastructures*, led to a Presidential Decision Directive (PDD-63) that was released May 22, 1998 (see CRS Report RL30153, *Critical Infrastructures: Background and Early Implementation of PDD-63*).

PDD-63 sets as a national goal the ability to protect critical infrastructures from intentional attacks (both physical and cyber) by 2003. It sets up an organizational structure for achieving this goal. Nineteen critical infrastructures (including four for which the federal government has the primary responsibility) have been identified. A lead agency has been assigned to each infrastructure. The lead agency is to work with

the appropriate private sector actors, and state and local governments in developing a national plan for their sector. Each plan is to include a vulnerability assessment, a remedial action plan, appropriate warning procedures, response strategies, reconstitution of services strategies, education and awareness program, research and development needs, intelligence enhancements, international cooperation, and any legislative and budgetary requirements.

A Critical Infrastructure Assurance Office has been set up in the Department of Commerce to help coordinate the development of these plans. A Critical Infrastructure Coordination Group, an interagency group, addresses interdependencies between agencies and sectors. The Group is chaired by a National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, and reports to the President through the Principal's Committee of the National Security Council on progress in implementing the PDD and the development of the national plans. The National Coordinator will also be the Executive Director of a National Infrastructure Assurance Council which will act as a Presidential advisory panel and include private, and state and local representatives.

PDD-63 also authorizes the Federal Bureau of Investigation to be the executive agent for a National Infrastructure Protection Center (NIPC). According to PDD-63, the NIPC is to act as the operational focal point for coordinating federal response to "attacks." The Directive also makes the NIPC the central federal point of contact for developing threat analyses, issuing warnings and sharing information regarding intrusions, hacking methods and fixes. The NIPC draws upon expertise found throughout the federal government. The PDD encourages the private sector to set up a parallel center to interact with the NIPC.

One of the capabilities that the Directive wants established is the ability to detect when an intrusion has occurred. An early concept for this envisioned intrusion detection hardware and software placed throughout the federal government's systems that would automatically feed network traffic data into a centralized location (such as the NIPC) that would analyze the data for tell-tale signs of intrusions. Dubbed the federal intrusion detection network (FIDNET), initial proposals raised privacy issues both inside and outside the Administration. Since then the proposal has changed. The network would be decentralized, each agency being responsible for installing intrusion detection hardware and software on its systems, analyzing the data, and only forwarding concerns if suspicious behavior has been detected. Those concerns and any supporting analysis would be forwarded first to the General Services Administration (GSA). The NIPC would only be contacted if it was determined that criminal activity had occurred.

In January 2000, the Administration released Version 1.0 of its National Plan for Information Systems Protection as called for in PDD-63. According to the Plan, agencies were to have completed initial vulnerability assessments of their most critical systems and budgeted for remedial actions in their FY2001 budget requests. Overall, the Administration states it is asking for $2.08 billion for protection of critical information infrastructures. This includes $25 million to support scholarships for service at accredited universities to help train a new generation of computer security experts and to offer certification programs for existing federal computer security experts to update and improve their skills.

From a law enforcement point of view, the federal computer fraud and abuse statute, 18 U.S.C. 1030, addresses protection of federal and bank computers, and computers used in interstate and foreign commerce. CRS Report 97-1025, *Computer Fraud & Abuse: An Overview of 18 U.S.C. 1030 And Related Federal Criminal Laws,* provides more information on the statute. In general, it prohibits trespassing, threats, damage, espionage, and using computers for committing fraud. While many experts believe these statutes to be sufficient to fight computer intrusions, many also believe that statues governing procedural issues (such pursuing hackers across jurisdictional lines in "cyberspace") need modification.

In December 1997, acknowledging the growing problem of crime on the Internet, the United States, Britain, Canada, France, Germany, Italy, Japan, and Russia agreed on steps to fight computer crimes: insure that a sufficient number of trained and equipped law enforcement personnel are allocated to fighting high-tech crime; establish high-tech crime contacts available on a 24-hour basis; develop faster ways to trace attacks coming through computer networks to allow for identification of the responsible hacker or criminal; where extradition of a criminal is not possible, devote the same commitment of time and resources to that prosecution that a victim nation would have devoted; preserve information on computer networks so computer criminals cannot alter or destroy electronic evidence; review legal systems to ensure they appropriately criminalize computer wrongdoing and facilitate investigation of high-tech crimes; and work with industry to devise new solutions to make it easier to detect, prevent and punish computer crimes.

The 106th Congress continues to be interested in the issue of computer security, especially as it affects critical infrastructures and national security. Congressional action in the first session consisted primarily of oversight hearings. A few bills were introduced. H.R. 2162 would amend 18 USC 1030, making it a federal crime to knowingly use without authorization someone else's domain name in sending email if damages to computers, computer systems, or networks result. H.R. 2816 and S. 1314 would establish Department of Justice grants to state and local authorities to help them investigate and prosecute computer crimes. H.R. 2413 would assign NIST a number of tasks, some of which NIST is already doing under more general authority, that would reinforce NIST's role in ensuring the security of the federal non-classified computer systems. Also, S. 1993 would modify the Paperwork Reduction Act and other relevant statutes concerning computer security of government systems, putting into statute a number of agency responsibilities some of which are already required by OMB Circular A-130, Appendix III. The bill was attached to the Senate version of the FY2001 defense authorization bill (S. 2549) in the second session.

The opening weeks of the second session of the 106th Congress witnessed the wide-spread denial-of-service attacks on major Web sites including Yahoo, Amazon, CNN, and E-Trade. A few months later, the world experienced the LoveBug virus, leading to the disruption of e-mail service around the world. A number of new bills have since been introduced that address different aspects of Internet security. In the House, H.R. 4210 would set up within the Office of the President an Office of Terrorism Preparedness that would include cyberterrorism in its jurisdiction. H.R. 4246 would address issues related to exchange of computer security information between firms and between the government and the private sector. The bill would make information contained on a cybersecurity Web site available only at the

discretion of the owners of the information and then it must be treated confidentially. It specifically exempts the information from the Freedom of Information Act and precludes the information from being used in any civil actions. It also frees the information contained on cybersecurity Web sites from anti-trust laws as long as the agreement governing information exchange on the site does not lead to non-competitive behavior. Finally, government working groups may be set up to interact with the private sector on computer security matters and not be considered federal advisory committees. H.R. 4347 would amend the statute related to installing pen registration and trap and trace devices in pursuit of criminal activity, would amend the criminal penalties for computer crimes, and would authorize the Department of Defense to provide research and development grants to study how to prevent cyberterrorism. H.R. 5024 would amend the Paperwork Reduction Act and the Clinger-CohenAct, establishing an Office of Information Policy headed by a government-wide Chief Information Officer. Many of the functions and responsibilities granted to the Director of Office of Management and Budget in the Paperwork Reduction Act would be transferred to the government-wide CIO, including those related to overseeing the development and implementation of information security policies, standards and guidelines. Also, the bill would establish within the Office of Information Policy an Office of Information Security and Technical Protection. The Director of this office would act as the principal adviser to the government-wide CIO on information security matters and would administer for the CIO the information security functions. The functions and responsibilities of the government-wide CIO and the individual agencies as laid out in this bill mirror those as laid out in S. 1993 mentioned above.

In the Senate, S. 2092 would make changes to the penalty section of 18 USC 1030(c), removing the dollar threshold for damages, redefining what may constitute damages, and considering findings of juvenile offenses as previous convictions under this section. S. 2430 would make similar amendments to 18 USC 1030. S. 2451 also addresses the penalties for computer crime and also calls for a National Cybersecurity Commission. S. 2448 is a broad bill that would address a number of issues. These include modifications to the definitions of computer crime and subsequent penalties, the issuance of pen registers and trap and trace devices to allow for cross jurisdictional investigations of specific computer crimes, and assistance to state and local governments to fight computer crime. The bill also addresses privacy issues, calls for a public awareness campaign regarding computer security, and outlines the Department of Justice's role in protecting critical infrastructures and in international computer crime enforcement. Another bill, S. 2545, would expand the Barry Goldwater Scholarship and Excellence in Education Program to include information protection technology.

Internet Privacy[4]

[4]See also CRS Report RS20035, *Internet Privacy—Protecting Personal Information: Overview and Pending Legislation*, which is updated more frequently than this report. For information on financial or medical records privacy, which are not Internet issues per se, see CRS Report RS20185 or CRS Issue Brief IB98002, respectively.

Many bills have been introduced in the 106th Congress dealing with Internet privacy in whole or in part (H.R. 313, H.R. 367, H.R. 369, H.R. 1685, H.R. 2882, H.R. 3321, H.R. 3560, H.R. 3770, H.R. 4049, H.R. 4311, H.R. 4611, H.R. 4857, H.R. 4987, S. 809, S. 854, S. 2063, S. 2328, S. 2448, S. 2554, S. 2699, S. 2857, S. 2871, S. 2876, S. 2924, and S.2928). In addition, amendments dealing with Internet privacy have been added to the FY2001 Treasury-Postal Appropriations bill (H.R. 4871) and the FY2001 Commerce, Justice, State Appropriations bill (H.R. 4690). The issue is discussed herein, but the bills are described in CRS Report RS 20035. Many of the bills require interactive computer services to allow consumers to "opt in" or "opt out" of having their personal identifiable information collected, used, or disseminated, or to notify consumers of their practices. Others address the rising number of cases of identity theft by restricting the use of Social Security numbers. One (H.R. 4049) has a quite different focus in that it would establish a privacy commission to study broad consumer privacy issues (including Internet privacy) for 18 months. Several hearings have been held in the 106th Congress: House Commerce subcommittee, July 13, 1999; House Government Reform subcommittee, May 15-16, 2000; House Judiciary subcommittee, May 27, 1999; Senate Commerce Committee, July 27, 1999, May 25, 2000, and June 13, 2000; and Senate Judiciary Committee, April 21, 1999 and May 25, 2000.

Consumer Identity Theft

The widespread use of computers for storing and transmitting information is thought to be contributing to consumer identity theft, in which one individual assumes the identity of another using personal information such as credit card and Social Security numbers. That belief is based primarily on anecdotal information, however. Some attribute the rise in reports of identity theft instead to carelessness by businesses in handling personally identifiable information, and by credit issuers that grant credit without proper checks, however. The Federal Trade Commission (FTC) has a toll free number (877-ID-THEFT) to help victims of identity theft.

A March 1997 Federal Reserve Board study, *Report to the Congress Concerning the Availability of Consumer Identifying Information and Financial Fraud,* concluded that there are insufficient data to draw conclusions about losses from this particular subset of financial fraud. Although the Board noted that anecdotal information suggested that type of fraud is increasing, it concluded that the losses are a small part of overall fraud losses and do not pose a significant threat to insured depository institutions.[5] A May 1998 General Accounting Office report, *Identity*

[5]Other types of computer fraud also are of concern. Computer networks offer a new mechanism for the commission of fraud and scams against unwitting consumers. Although the types of fraud and scams that have been identified on the Internet are not new, perpetrators have easy access to a wide audience via the Internet. On July 14, 1998, the Federal Trade Commission (FTC) released a list of the 12 most common scams found in unsolicited commercial electronic mail [http://www.ftc.gov./opa/9807/dozen.htm]. The Securities and Exchange Commission (SEC) established a new Office of Internet Enforcement to handle Internet fraud cases in July 1998. The SEC reported that since 1995 it had brought more than 30 cases involving Internet-related securities fraud and now was receiving 120 complaints daily about Internet-related potential securities violations. Computer fraud is addressed by (continued...)

Fraud: Information on Prevalence, Cost, and Internet Impact is Limited (GAO/GGD-98-100BR), also found that few statistics are available on identity fraud, but that many of the individuals it interviewed believe the Internet increases opportunities for identity theft and fraud.

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. Subsequent hearings (April 22, 1999, House Commerce; March 7 and July 12, 2000, Senate Judiciary) have discussed continuing issues and new legislation has been introduced in the 106th Congress. H.R. 4311 (Hooley)/S.2328 (Feinstein) would impose requirements on credit card issuers, consumer reporting agencies, and individual reference services to reduce the likelihood of identity theft. H.R. 4611 (Markey)/S. 2699 (Feinstein) would regulate the sale and use of Social Security numbers (SSNs); the bills were introduced at the request of Vice President Gore. H.R. 4857 (Shaw)/S. 2876 (Bunning) prohibit the sale of and otherwise protect SSNs. H.R. 4857 has been marked up by a House Ways and Means subcommittee.

In a related matter, a Senate Governmental Affairs subcommittee held a hearing May 19, 2000 on how the Web makes it easier to produce and distribute false identification documents (IDs). S. 2924 (Collins) would update existing law against selling or distributing false IDs to include those sold or distributed through computer files and templates, and would make it easier to prosecute such crimes.

Individual Reference or "Look-Up" Services

The Federal Trade Commission (FTC) held a public workshop in June 1997 that focused on the collection of information about consumers by companies that operate computerized databases of personal information, called "individual reference services" or "look-up services." Just prior to the workshop, several of those companies announced voluntary principles they would follow in the future to protect consumer privacy. In December 1997, the FTC released a report on the workshop and the industry principles: *Individual Reference Services: A Report to Congress* [http://www/ftc/gov/opa/9712/inrefser.htm]. Among the principles are that individual reference services will not distribute to the general public non-public information such as Social Security numbers, birth dates, mother's maiden names, credit histories, financial histories, medical records, or any information about children. Look-up services may not allow the general public to run searches using a Social Security number as a search term or make available information gathered from marketing transactions. Also, consumers will be allowed to obtain access to the non-public

---

[5](...continued)
18 U.S.C. 1030 and the United States and seven other countries agreed in December 1997 to coordinate their efforts at fighting computer crime, including fraud. Hearings have been held on Internet fraud: Senate Governmental Affairs Committee, February 10, 1998 and March 22 and 23, 1999; and House Commerce Committee, June 25, 1998. Three bills are pending in the 106th Congress: H.R. 612 (Weygand)and S. 699(Wyden) focus on protecting senior citizens against telemarketing fraud, including over the Internet; S. 1015 (Schumer) seeks to protect online investors.

information maintained about them and to "opt-out" of that non-public information. The FTC noted that the principles did not address all areas of concern and made a number of recommendations accordingly. The principles led to voluntary industry guidelines that took effect on January 1, 1999.

Collection of Data by Web Site Operators

The Internet ("online") privacy debate is over whether industry self regulation or legislation is the best approach to assuring consumer privacy rights. Although Congress and the Clinton Administration both prefer self regulation, the 105th Congress passed legislation to protect the privacy of children under 13. Not only are there concerns about information children might divulge about themselves, but about their parents, in response to questions asked at various Web sites. Congress therefore passed and the President signed into law the Children's Online Privacy Protection Act (COPPA) as Title XIII of Division C of the FY1999 Omnibus Consolidated and Emergency Supplemental Appropriations Act (P.L. 105-277). The law requires operators of World Wide Web sites to obtain verifiable parental consent before collecting, using, or disseminating information about children under 13, and allowing parents to "opt out" of dissemination of information already collected about that child. The FTC issued a final rule [http://www.ftc.gov/privacy/index.html] implementing the Act on October 20, 1999, which became effective April 21, 2000 (see CRS Report RS20035 for further information).

Passage of the law followed years of debate on the need for legislation versus relying on industry self regulation. In its July 1997 report, *A Framework for Global Electronic Commerce,* the Clinton Administration endorsed industry self regulation for protecting consumer Internet privacy, but stressed that if industry did not self-regulate effectively the government might have to step in, particularly regarding children. On May 14, 1998, Vice President Gore called for an "electronic bill of rights" to protect consumers' privacy. He encouraged Congress to pass medical records privacy legislation (see CRS Issue Brief IB98002), and announced the establishment of an "opt-out" Web site [http://www.consumer.gov] by the FTC to allow individuals to indicate they do not wish personal information passed on to others. At a June 23-24, 1998 "summit" on Internet privacy, Secretary of Commerce Daley warned industry that the Administration would seek legislation to protect all online consumers if industry did not accelerate its privacy protection efforts in general. On July 31, 1998, Vice President Gore addressed a wide range of privacy issues, reiterating his call for Congress to pass legislation requiring parental consent before information is collected about children under 13. The Vice President renewed the Administration's emphasis on industry self regulation, but noted the test of success would be the degree of industry participation.

In a July 17, 2000 speech, White House Chief of Staff Podesta proposed legislation to update existing wiretap laws covering telephone and other types of communications to include electronic communications such as e-mail, and enhance electronic privacy and civil liberties. At about that time, though, controversy erupted over an FBI "e-mail sniffing" program called Carnivore that the FBI, with a court order, can install on Internet Service Providers' equipment to intercept e-mail. The extent to which Carnivore can differentiate between e-mail involving a subject of an investigation and other people's e-mail is of considerable debate, with critics claiming

that Carnivore violates the privacy of innocent e-mail users. A House Judiciary subcommittee held a hearing on Carnivore on July 24. Legislation (H.R. 4987, Barr) to *inter alia* require law enforcement to report on its use of e-mail intercepts and block the use of electronic evidence in court if it is obtained illegally was introduced July 27.

Another controversy, dubbed "Cookiegate" in the press, has arisen over federal agencies' use of computer "cookies"(small text files placed on users' computers when they access a particular Web site) to track activity at their Web sites. Federal agencies have been directed by the President and the Office of Management and Budget (OMB) to ensure that their information collection practices adhere to the Privacy Act of 1974. In June 2000, however, the White House announced that it had just learned that contractors for the Office of National Drug Control Policy (ONDCP) had been using cookies to collect information about those using ONDCP's Web site during an anti-drug campaign wherein users clicking on anti-drug ads on various Web sites were taken to an ONDCP site. Cookies then were placed on users' computers to count the number of users, what ads they clicked on, and what pages they viewed on the ONDCP site. The White House directed ONDCP to cease using cookies, and OMB issued a memorandum reminding agencies to post and comply with privacy policies and detailing the limited circumstances under which agencies should collect personal information. Subsequently, the House adopted an Inslee amendment to the FY2001 Treasury-Postal Appropriations bill (H.R. 4871) requiring Inspectors General of agencies funded by the bill to report to Congress on any activity taken to monitor individuals who access any Internet site of their agencies, and a Frelinghuysen amendment prohibiting funding in the bill from being used to collect information on individuals using a federal Internet site.

The FTC has been very active on Internet privacy issues for several years. Two FTC surveys of Web sites, in December 1997 and June 1998, to determine how the industry was responding to privacy concerns resulted in statistics showing many Web sites collecting personally identifiable information but few disclosing their information collection practices or posting privacy policies. Frustrated at the survey results, the FTC announced on June 4, 1998 that it would seek legislation protecting children's privacy on the Internet by requiring parental permission before a Web site could request information about a child. COPPA was enacted four months later.

Two industry-sponsored studies conducted by Dr. Mary Culnan of Georgetown University [http://www.msb.edu/faculty/culnanm/gippshome.html] in the spring of 1999 found a larger percentage (66%) of the Web sites in those surveys posting a privacy policy or an information practice statement, up from 14% in the 1998 FTC survey, but only 36% posted both types of disclosures. Of the top 100 Web sites, 93% posted either type of disclosure, but only 20% provided the four elements of fair information practices (notice, choice, access, and security). The Georgetown statistics thus provided ammunition to both sides in the debate. For its part, the FTC concluded that additional legislation was not needed at that time.

However, in May 2000, the FTC released another survey, entitled *Privacy Online: Fair Information Practices in the Electronic Marketplace* [http://www/ftc/gov/opa/2000/05/privacy2k.htm]. The survey found that only 20% of randomly visited Web sites with at least 39,000 unique monthly visitors, and 42%

of the 100 most popular Web sites, had implemented all four fair information practices (notice, choice, access, and security). The FTC concluded that self regulation had not yet established "a significant presence on the Web." The FTC voted 3-2 to propose legislation that would allow it to establish regulations requiring Web site operators to follow the four fair information practices. The close vote underscored the controversial nature of the FTC's reversal of position, which was further elucidated at a Senate Commerce Committee hearing on May 25.

The Internet industry prefers self regulation, and one action it took to demonstrate its intention to self regulate was the formation of the Online Privacy Alliance (OPA). OPA developed a set of privacy guidelines and its members are required to adopt and implement posted privacy policies. The Better Business Bureau (BBB), TRUSTe, and WebTrust, among others, have established "seals" for Web sites. To display a seal from one of those organizations, a Web site operator must agree to abide by certain privacy principles (some of which are based on the OPA guidelines), a complaint resolution process, and to being monitored for compliance. Advocates of self regulation argue that these seal programs demonstrate industry's ability to police itself. Advocates of legislation argue that while the seal programs are useful, they do not carry the weight of law, limiting remedies for consumers whose privacy has been violated. They also point out that while a site may disclose its privacy policy, that does not necessarily equate to having a policy that protects privacy. Two studies, one by the Center for Democracy and Technology [http://www.cdt.org/privacy/990727privacy.pdf] and one by the Electronic Privacy Information Center [http://www.epic.org/reports/surfer-beware3.html] explore that viewpoint.

Public interest groups have become particularly concerned about online profiling where companies collect data about what Web sites are visited by a particular user and develop profiles of that user's preferences and interests for targeted advertising. Following a one-day workshop on online profiling, FTC issued a two-part report in the summer of 2000 that also heralded the announcement by a group of companies that collect such data, the Network Advertising Initiative (NAI), of self-regulatory principles. The FTC also called on Congress, however, to enact legislation to ensure consumer privacy vis a vis online profiling.

European Data Directive

One factor in the U.S. debate over the merits of self regulation versus legislation is the need for the United States to address policies adopted in Europe concerning data privacy. The European Union (EU) adopted a policy in 1995 referred to as the "European data directive" that requires member countries to pass laws prohibiting the transfer of personal data to countries that are not members of the EU ("third countries") unless the third countries ensure an "adequate level of protection" for personal data. The directive went into force on October 25, 1998. Since the United States does not have such laws, the U.S. Department of Commerce (DOC) negotiated with the EU to accept "safe harbor" certifications developed by DOC and U.S. industry whereby U.S. companies can satisfy the intent of the EU data directive through adhering to certain self regulatory principles. After two years of negotiations, the agreement was approved by the European Commission (the "executive arm" of the EU) in May 2000. The European Parliament, consisting of elected representatives

of the EU countries, subsequently disapproved it, however, asking for further negotiations with the United States. The European Parliament's decision was not binding on the EC, though, and the EC decided to proceed with implementing the agreement after conveying to the United States the concerns expressed by the European Parliament. The final safe harbor documents are at [http://www.ita.doc.gov/td/ecom/menu.html].

Protecting Children from Unsuitable Material and Sexual Predators[6]

Concern is growing about what children are encountering over the World Wide Web, particularly in terms of indecent material or contacts with strangers who intend to do them harm. The private sector has responded by developing filtering and tracking software to allow parents either to prevent their children from visiting certain Web sites or to provide a record of what sites their children have visited.

Congress passed the Communications Decency Act (CDA) as part of the 1996 Telecommunications Act (P.L. 104-104). Among other things, CDA would have made it illegal to send indecent material to children via the Internet. In June 1997, the Supreme Court overturned the portions of the CDA dealing with indecency and the Internet. (Existing law permits criminal prosecutions for transmitting obscenity or child pornography over the Internet.) Congress passed a replacement law, the Child Online Protection Act, in 1998, but it is being challenged in the courts (see below).

Prohibiting Access by Children to Material That is "Harmful to Minors"

Congress passed the Child Online Protection Act (COPA) as part of the Omnibus Appropriations Act (P.L. 105-277, Title XIV of Division C). The law prohibits commercial distribution of material over the Web to children under 17 that is "harmful to minors." Web site operators are required to ask for a means of age verification such as a credit card number before displaying such material. It replaces provisions of the 1996 Communications Decency Act that were overturned by the Supreme Court. By limiting the language to commercial activities and using the court-tested "harmful to minors" language instead of "indecent" as was used in the 1996 Act, the sponsors had hoped to have drafted a law that would survive court challenges. The American Civil Liberties Union (ACLU) and others filed suit against the provisions regarding the "harmful to minors" language in the new law in the U.S. District Court for the Eastern District of Pennsylvania on October 22, the day after President Clinton signed the bill into law. A temporary restraining order preventing enforcement of the relevant sections of the Act was issued in November 1998 and a preliminary injunction was issued in February 1999. The Department of Justice is appealing the

---

[6]See also CRS Report RS20036, *Internet—Protecting Children from Unsuitable Material and Sexual Predators: Overview and Pending Legislation*, which is updated more frequently than this report.

ruling. (See CRS Report 98-670 A, *Obscenity, Child Pornography, and Indecency: Recent Developments and Pending Issues.*)

COPA establishes a Commission on Online Child Protection to conduct a one-year study of technologies and methods to help reduce access by children to material on the Web that is harmful to minors. The Commission is composed of 16 industry members appointed by the Republican and Democratic congressional leaders plus one ex officio representative each from the Federal Trade Commission (FTC) and Departments of Commerce and Justice. The final members were appointed on October 19, 1999. Originally, the Commission was given one year to complete its task, but since naming the members took longer than expected Congress extended the Commission's life for another year in the FY2000 Consolidated Appropriations Act (P.L. 106-113). Congress did not allocate any funding for the Commission's operations, however, and although the original law established it under the auspices of the National Telecommunications and Information Administration (NTIA, part of the Department of Commerce) that section was eliminated when the Commission's lifetime was extended. The Commission now operates independently [http://www.copacommission.org] and has held several meetings. Separately, P.L. 105-314 requires the National Research Council to prepare a study within two years on the capabilities of current computer-based control technologies to control the electronic transmission of pornographic images and identify needed research to develop such technologies and any inherent, operational, or constitutional impediments to their use.

Filtering Software

A particular focus of the debate over how to protect children from unsuitable material on the Internet has been whether to require schools and libraries to use filtering technology to block objectionable Web sites. Policies adopted by local communities reflect the spectrum of attitudes on this topic. Some are choosing to allow children to use computers at local libraries only with parental permission, some are using filtering software, and others are choosing no restrictions.

Software to block access to Web sites or e-mail addresses has existed for many years (commercial products include Cyber Patrol, Cyber Sitter, Net Nanny, Net Shepard, and SurfWatch). Other products (such as Net Snitch) do not prohibit access to sites, but maintain a record that a parent can review to know what sites a child has visited. Some filtering products screen sites based on keywords, while others use ratings systems based on ratings either by the software vendor or the Web site itself. Both types of ratings are becoming more available as industry attempts to self-regulate to stave off governmental regulation. Existing filtering software products have received mixed reviews, however, because they cannot effectively screen out all objectionable sites on the ever-changing Web, or because they inadvertently screen out useful material.

Some privacy groups object to filtering software because of the amount of useful information to which it denies access. A November 1997 report on filtering software was released by the Electronic Privacy Information Center (EPIC) entitled *Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet* [http://www2.epic.org/reports/filter-report.html]. EPIC tested a filtering

program called Net Shepard, searching the Web for sites it expected to be useful to and suitable for children. For example, EPIC searched for Web sites about the "American Red Cross" (entered into the search engine in quotes to ensure that only items with that exact set of words in that order would be returned) with and without Net Shepard activated. EPIC reported that Net Shepard prevented access to 99.8% of the sites. From this and other similar examples, EPIC concluded that in the effort to protect children from a small amount of unsuitable material, they were being denied access to a large amount of suitable information. Many privacy advocates also feel that filtering is a form of censorship. Other critics object to the fact that a parent would not know specifically what sites or words a particular software product was blocking out. Critics of federally mandated filtering argue that schools and libraries should adopt "acceptable use" policies instead, where agreements are reached with children as to what their conduct should be on the Internet. The American Library Association, the National Education Association, and the Center for Democracy and Technology are among the groups that oppose federally mandated filtering for schools and libraries.

The 105th Congress included a provision in the Child Online Protection Act requiring interactive computer services to advise customers that parental control protections (hardware, software, or filtering services) are commercially available.

Many ISPs already provide parents with tools and information to help them guide their children. On May 5, 1999, Vice President Gore held a press conference with representatives of the Internet industry to announce that by July 1999 from "any access point" on the Internet, parents and children would be just "one click away" from a resource guide called a Parents' Protection Page providing "tools, tips, and resources for safe surfing on the net." (White House press release May 5, 1999, *Vice President Gore Announces the Parents' Protection Page.*) On July 29, a coalition of major Internet companies (including AOL, AT&T, MCI, Disney, Microsoft, and Yahoo) and other organizations (including the National Center for Missing and Exploited Children, Enough is Enough, and Center for Democracy and Technology) debuted a new Web site [http://www.GetNetWise.org] that provides links to such tools and information. Rather than the site being "one click away" from "any access point" on the Web, the companies that participated in its creation say they will establish links to it from their own sites or recompile the information and present it themselves. They assert that almost 95% of Web traffic flows through their sites (*New York Times* online, July 30, 1999). The site appears to replace an earlier industry-sponsored Web site (AmericaLinksUp) that provided parental assistance. Since much of the information on the site pertains to filtering products, critics of filtering are also generally critical of the Web site. They emphasize that direct parental involvement is the best method for protecting children who use the Web.

A major focus of the continuing debate in Congress is whether to require schools and/or libraries that receive federal funding under Title III of the Elementary and Secondary Education Act, or through federal "E-rate" funds under universal service, to use filtering technology to screen out objectionable Web sites. (For information on universal service and the E-rate, see CRS Issue Brief IB98040, *Telecommunications Discounts for Schools and Libraries: the "E-Rate" Program and Controversies).*

Many bills are pending in the 106th Congress, but attention is currently focused on language in the House- and Senate-passed versions of the FY2001 Labor-HHS appropriations bill, H.R. 4577. The language is quite different in the House and Senate versions, and three amendments adopted by the Senate differ among each other. CRS Report RS20036 describes these provisions in more detail, but a brief synopsis follows.

In the version of H.R. 4577 that passed the House on June 14, 2000, schools receiving funds under title III of the Elementary and Secondary Education Act (ESEA) for purchasing computers used to access the Internet or paying direct costs associated with accessing the Internet must install filters on any computer to which minors have access. The filter must block material that is obscene, child pornography, and material harmful to minors. Local educational agencies or schools specifically are not prohibited from filtering other materials. The House language does not address libraries. (The provision is the same as language in H.R. 4141, the "Education OPTIONS," bill as reported by the House Education and the Workforce Committee (H. Rept. 106-608.)

By contrast, the Senate adopted language during floor debate on H.R. 4577 on June 27, 2000, placing various requirements on schools and libraries receiving E-rate funding and on Internet Service Providers (ISPs). First, the Senate adopted a McCain amendment requiring schools and libraries receiving E-rate funding to select a technology for computers that have Internet access to filter or block material that is obscene and child pornography, and enforce a policy ensuring its operation when the computers are being used by minors. Local school officials also are *permitted* to use the technology to filter or block access to other materials they determine to be "inappropriate for minors," while libraries are *required* to do so. Libraries also must block child pornography during any use of the computer, not only when a computer is being used by minors. Determination of what material is to be filtered or blocked would be made by local officials. A Hatch/Leahy amendment to the McCain amendment was also adopted that requires ISPs with more than 50,000 subscribers to provide filtering software or blocking systems to all residential customers at the time they sign up for service (This provision originally had been adopted by the Senate as an amendment to the juvenile justice bill, S. 254, in May 1999.). The software or system must be provided for free or at a cost no higher than what the ISP paid for it.

The Senate then adopted a Santorum amendment (based on S. 1545) that would permit schools and libraries to choose between using filtering technology or having "acceptable use"policies, called "Internet use" policies in the amendment. Filtering systems must filter or block access to matter considered to be inappropriate for minors as determined by the school board or library or other local authority. Internet use policies must address specific matters identified in the amendment and reasonable public notice of the policy must be provided and at least one public hearing or meeting conducted.

Sexual Predators on the Internet

The 106th Congress continues to debate issues concerning how to protect children from sexual predators on the Internet. Because conversations can take place

anonymously on the Internet, a child may not know that (s)he is talking with an adult. The adult may persuade the child to agree to a meeting, with tragic results Representative Johnson (CT) has introduced H.R. 1159, the Protection of Children from On-Line Predators and Exploitation Act. The bill would increase FY2000 funding for the Customs Service's Child Pornography/Child Sexual Exploitation Program from $2.4 million to $10 million and provide greater wiretap authority in cases where people are suspected of traveling across international borders to engage in sexual acts with juveniles. H.R. 640 (Lampson) would authorize $5 million for each of the fiscal years 2000, 2001, 2002, and 2003 for the U.S. Customs Cybersmuggling Center.

The 105th Congress also was concerned about sexual predators using the Internet to entice children, passing H.R. 3494, the Protection of Children from Sexual Predators Act, to address those and other non computer-related issues related to protecting children from sexual predators. The bill was signed into law on October 30, 1998 (P.L. 105-314).

Separately, a provision (section 122 of General Provisions—Justice Department) in the FY1999 Omnibus Appropriations Act (P.L. 105-277) gives the FBI administrative subpoena authority in cases involving a federal violation related to sexual exploitation and abuse of children. The provision is intended to make it easier for the FBI to gain access to Internet service provider records of suspected sexual predators.

The FY1999 Omnibus Appropriations Act (P.L. 105-277) set aside $2.4 million in the Customs Service appropriation to double the staffing and resources for the child pornography cybersmuggling initiative and provided $1 million in the Violent Crime Reduction Trust Fund for technology support for that initiative. The FY2000 Treasury-Postal Service appropriations act (P.L. 106-58) includes $4 million for the Customs Service's Cybersmuggling Center.

Unsolicited Commercial Electronic Mail ("Junk E-Mail" or "Spam")[7]

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

In 1991, Congress passed the Telephone Consumer Protection Act (P.L. 102-243) that prohibits, *inter alia*, unsolicited advertising via facsimile machines, or "junk fax" (see CRS Report 98-514, *Telemarketing Fraud: Congressional Efforts to Protect Consumers*). Many question whether there should be an analogous law for computers, or at least some method for letting a consumer know before opening an e-mail message whether or not it is unsolicited advertising and to direct the sender to cease transmission of such messages. At a November 3, 1999 hearing of the House Commerce telecommunications subcommittee, a representative of SBC Internet Services, a subsidiary of SBC Communications, Inc., stated that 35% of all the e-mail transmitted over SBC's Internet systems in its Pacific Bell and Southwestern Bell regions is UCE.

Opponents of junk e-mail such as the Coalition Against Unsolicited Commercial Email (CAUCE) argue that not only is junk e-mail annoying, but its cost is borne by consumers, not marketers. Consumers are charged higher fees by Internet service providers that must invest resources to upgrade equipment to manage the high volume of e-mail, deal with customer complaints, and mount legal challenges to junk e-mailers. According to the May 4, 1998 issue of Internet Week, $2 of each customer's monthly bill is attributable to spam [http://www.techweb.com/se/directlink.cgi?INW19980504S0003]. Some want to prevent bulk e-mailers from sending messages to anyone with whom they do not have an established business relationship, treating junk e-mail the same way as junk fax. Proponents of unsolicited commercial e-mail argue that it is a valid method of advertising. The Direct Marketing Association (DMA), for example, argues that instead of banning unsolicited commercial e-mail, individuals should be given the opportunity to notify the sender of the message that they want to be removed from its mailing list — or "opt-out." In January 2000, the DMA launched a new service, the E-mail Preference Service, where any of its members that send UCE must do so through a special Web site where consumers who wish to "opt out" of receiving such mail can register themselves [http://www.e-mps.org]. Each DMA member is required to check its list of intended recipients and delete those consumers who have opted out. While acknowledging that the service will not stop all spam, the DMA considers it "part of the overall solution" [http://www.the-dma.org/aboutdma/release4.shtml]. Critics argue that most spam does not come from DMA members, so the DMA plan is insufficient.

---

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

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

Although the House and Senate each passed legislation addressing the unsolicited commercial e-mail problem, no bill ultimately cleared the 105th Congress. Several bills in the 106th Congress address the issue (H.R. 1685, H.R. 1686, H.R. 1910, H.R.2162, H.R. 3024, H.R. 3113, S. 759, S. 2448, and S. 2542), and one, H.R. 3113, has passed the House. See CRS Report 20037 for an explanation of that bill's provisions. In addition, some states are passing their own legislation. According to the National Conference of State Legislatures, as of March 2000, 15 states had enacted such laws and 16 introduced spam bills during their 2000 legislative sessions. S. 759 would preempt state laws regarding spam.

Internet Domain Names[8]

The 106th Congress continues to monitor issues related to the Internet domain name system (DNS). Internet domain names were created to provide users with a simple location name for computers on the Internet, rather than using the more complex, unique Internet Protocol (IP) number that designates their specific location. As the Internet has grown, the method for allocating and designating domain names has become increasingly controversial.

The Internet originated with research funding provided by the Department of Defense Advanced Research Projects Agency (DARPA) to establish a military network. As its use expanded, a civilian segment evolved with support from the National Science Foundation (NSF) and other science agencies. While there are no formal statutory authorities or international agreements governing the management and operation of the Internet and the DNS, several entities have played key roles in the DNS. The Internet Assigned Numbers Authority (IANA) makes technical decisions concerning root servers, determines qualifications for applicants to manage country code Top Level Domains (TLDs), assigns unique protocol parameters, and manages the IP address space, including delegating blocks of addresses to registries around the world to assign to users in their geographic area. IANA operates out of the University of Southern California's Information Sciences Institute and has been funded primarily by the Department of Defense.

Prior to 1993, NSF was responsible for registration of nonmilitary generic Top Level Domains (gTLDs) such as .com, .org, .net, and .edu. In 1993, the NSF entered into a 5-year cooperative agreement with Network Solutions, Inc. (NSI) to operate

---

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

Internet domain name registration services. In 1995, the agreement was modified to allow NSI to charge registrants a $50 fee per year. Since the imposition of fees in 1995, criticism arose over NSI's sole control over registration of the gTLDs. In addition, there was an increase in trademark disputes arising out of the enormous growth of registrations in the .com domain. With the cooperative agreement between NSI and NSF due to expire in 1998, the 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 Department of Commerce (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." Accordingly, Internet constituencies from around the world held a series of meetings during the summer of 1998 to discuss how the New Corporation might be constituted and structured. On October 2, 1998, the Department of Commerce accepted a proposal, authored primarily by IANA and NSI, for an Internet Corporation for Assigned Names and Numbers (ICANN). Nine members of ICANN's interim board were chosen (four Americans, three Europeans, one from Japan, and one from Australia). The proposal was criticized by some Internet stakeholders, who claimed that ICANN did not adequately represent a consensus of the entire Internet community. On November 25, 1998, DOC and ICANN signed an official Memorandum of Understanding, 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. On October 6, 1998, DOC and NSI announced an extension of the Cooperative Agreement between the federal government and NSI through September 30, 2000. 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 will permit multiple registrars to provide registration services within the .com, .net., and .org gTLDs. On April 21, 1999, ICANN announced the accreditation of five companies as participants in the test bed phase of the Shared Registration System (SRS). The test bed phase ended on November 30, 1999. All accredited registrars are now eligible to participate in the Shared Registration System. To date, 127 companies have either been accredited as a registrar by ICANN, or have qualified for accreditation; currently, 59 registrars are operational. NSI 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. Of particular controversy

was NSI's refusal to sign ICANN's accreditation agreement. On September 28, 1999, after nearly a year of negotiations, DOC, NSI, and ICANN announced a series of formal agreements. NSI agreed to sign an accreditation agreement with ICANN, but with certain limits and conditions placed on ICANN decisions that could affect NSI's business. NSI will retain control of the .com registry for at least four years; if ownership of NSI's registry and registrar operations is fully separated within 18 months (via spinoff or sale to a third party for example), the term would be extended for four additional years. NSI and all accredited registrars will provide public access to the full database of registered domain names (the "WhoIs" database). Competing registrars will pay NSI a wholesale price of $6 per registered name per year. Finally, NSI will pay ICANN $1.25 million upon signing the agreement, and agrees to approve an ICANN registrar fee policy as long as NSI's share does not exceed $2 million.

While the agreement was hailed by DOC, NSI, and ICANN, opposition was voiced by competing registrars, who asserted that the agreement gives NSI too many advantages in the competition for new registrations and renewals of existing ones. Others objected to the limits placed on ICANN with regard to making decisions that might affect NSI. At its November 1999 board meeting, ICANN agreed to modifications of the agreement which addressed some of the concerns raised. On November 10, 1999, ICANN, NSI, and DOC formally signed the agreements.

Until the full transition to a private sector controlled DNS system is completed, the Department of Commerce remains responsible for monitoring the extent to which ICANN satisfies the principles of the White Paper as it makes critical DNS decisions. Congress remains keenly interested in how the Administration manages and oversees the transition to private sector ownership of the DNS. The conference report (H.Rept. 106-479) accompanying the FY2000 Consolidated Appropriations Act (P.L. 106-113, signed November 29, 1999) directs the General Accounting Office (GAO) to review the legal basis and authority for DOC's relationship with ICANN (including the possible transfer of the authoritative root server to private sector control), the possibility of shifting federal oversight responsibilities from NTIA to the National Institute of Standards and Technology (NIST), and the adequacy of existing security arrangements safeguarding critical hardware and software underlying the DNS. The GAO report, released on July 7, 2000, concluded that the DOC does have legal authority to enter into its current agreements and cooperative activities with ICANN. GAO noted that while it is unclear whether DOC has the authority to transfer control of the authoritative root server to ICANN, the Department has no current plans to do so.

Two issues currently being addressed by ICANN are the addition of new top level domains and the election of At-Large Board members. At its July 16, 2000 meeting in Yokohama, the ICANN Board of Directors adopted a policy for the introduction of new top-level domains (TLDs). Additional gTLDs will expand the number of domain names available (beyond .com, .net., and .org) for registration by the public. The policy involves a process in which those interested in operating or sponsoring new TLDs may apply to ICANN. After reviewing the applications, ICANN will select applicants that will enter a negotiation process with ICANN. It is anticipated that this policy will lead to new TLDs coming into operation early in the year 2001.

Regarding the composition of ICANN's board of directors, ICANN bylaws call for an international and geographically diverse 19-member board of directors, composed of a president, nine at-large members, and nine members nominated by three Supporting Organizations. At ICANN's March 2000 meeting in Cairo, the sitting board agreed to a plan whereby five At-Large board members, one from each of five geographic regions of the world, will be directly elected by November 1, 2000. Eligible to vote is anyone over 16 years old who has an active email and postal address, and registers as an ICANN member. The registration period ended on July 31, 2000, with 158,000 people registering to vote. On August 1, the Nominating Committee released the names of 18 nominees; during August, additional individuals can be nominated by receiving support from 2% of registered voters in his or her region. The election will take place from October 1 - 10. Meanwhile, the sitting board will conduct a study to determine how to select the remaining four At-Large board members.

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

The increase in conflicts over property rights to certain trademarked names has resulted in a number of lawsuits. Under previous policy, NSI did not determine the legality of registrations, but when trademark ownership was demonstrated, placed the use of a name on hold until the parties involved could resolve the domain name dispute. 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. As of August 18, 2000, 1492 proceedings (encompassing the disposition of 2608 domain names) have been initiated.

Meanwhile, the 106th Congress took action, passing the Anticybersquatting Consumer Protection Act (incorporated into P.L. 106-113, the FY2000 Consolidated Appropriations Act). The Act gives courts the authority to order the forfeiture, cancellation, and/or transfer of domain names registered in "bad faith" that are identical or similar to trademarks. The bill would also provide for statutory civil

damages of at least $1,000, but not more than $100,000, per domain name identifier. The legislation was supported by corporate entities and others who wish to protect their trademarks and names from abusive or bad-faith domain name registrations. The legislation was opposed by civil libertarians who assert that the law threatens free expression on the Internet. The Clinton Administration also opposed the legislation, arguing that ICANN's dispute resolution procedure should not be circumvented.

Finally, Congress remains concerned about the disposition of the Intellectual Infrastructure Fund. The rapid growth of domain name registrations and the associated increase in costs to NSF led to the decision to charge a registration and maintenance fee to domain name holders. In 1995, NSI was authorized through an amendment to the cooperative agreement to charge $100 to initially register a domain name and $50 a year to maintain it in the database. According to the contract, 70% of the monies collected were to be retained by NSI to cover its costs; the remaining 30% were deposited by NSI in an account for the purpose of reinvestment in the Intellectual Infrastructure Fund (IIF) of the Internet. As of March 31, 1998, when fee collection was discontinued, approximately $60 million had been collected. The VA/HUD/Independent Agencies FY1998 Appropriations Act (P.L. 105-65) directed NSF to credit up to $23 million of the funds to NSF's Research and Related Activities account for Next Generation Internet activities. A class action suit filed in October 1997 challenged NSF's authority to allow NSI to collect fees. A May 14, 1999 ruling by the U.S. Court of Appeals upheld an earlier court ruling that affirmed the legality of the IIF. Meanwhile, the Home Page Tax Repeal Act (H.R. 2797/S. 705), introduced by Representative Terry and Senator Ashcroft, seeks to ensure refunds of all fees collected into the IIF. On March 24, 1999, the Basic Research Subcommittee of the House Committee on Science held a hearing on Home Page Tax Repeal Act. On November 2, 1999, the Basic Research Subcommittee marked up H.R. 2797.

Broadband Internet Access[9]

Broadband or high-speed Internet access is provided by a series of technologies that give users the ability to send and receive data at volumes and speeds far greater than current Internet access over traditional telephone lines. In addition to offering speed, broadband access provides a continuous "always on" connection (no need to dial-up) and a "two-way" capability, that is, the ability to both receive (download) and transmit (upload) data at high speeds.

Broadband access, along with the content and services it might enable, has the potential to transform the Internet—both what it offers and how it is used. For example, a two-way high speed connection could be used for interactive applications such as online classrooms, showrooms, or health clinics, where teacher and student (or customer and salesperson, doctor and patient) can see and hear each other through their computers. An "always on" connection could be used to monitor home security, home automation, or even patient health remotely through the Web. The high speed and high volume that broadband offers could also be used for bundled services, where for example, cable television, video on demand, voice, data, and other services are all

[9]See also CRS Issue Brief IB10045, *Broadband Internet Access: Background and Issues*, which is updated more frequently than this report.

offered over a single line. In truth, it is possible that many of the applications that will best exploit the technological capabilities of broadband, while also capturing the imagination of consumers, have yet to be developed.

Many offices and businesses now have Internet broadband access. A major remaining challenge is providing broadband over "the last mile" to consumers in their homes. Currently, between 2.5 and three million homes in the United States (between 2 and 3% of all households) are wired for broadband access. However, the changeover to residential broadband has begun, as companies have started to offer different types of broadband service in selected locations. Indeed, throughout the telecommunications and information industry, companies have been investing, acquiring, and merging in order to position themselves for what is felt to be a coming explosion in broadband Internet use. No one knows exactly how many consumers will be willing to pay for broadband service. Current costs to consumers range from about $40 and upward per month, plus up to several hundred dollars for installation and equipment. According to research from Juniper Communications, broadband users will number about 5.5 million through 2000, compared to 43.6 million dial-up users, and by 2002, broadband penetration will be 11.7 million users or 19% of online households.

Broadband Technologies

There are multiple transmission media or technologies which can be used to provide broadband access. These include cable modem technology, an enhanced telephone service called digital subscriber line (DSL), satellite technology, terrestrial wireless technologies, and others. Cable modems and DSL are generally acknowledged by many observers as the most promising technologies for providing broadband access, at least within the next couple of years. Both require the modification of an existing physical infrastructure that is already connected to the home (i.e. cable television and telephone lines). Each technology has its respective advantages and disadvantages, and will likely compete with each other based on performance, price, quality of service, geography, user friendliness, and other factors.

According to Kinetic Strategies Inc., an estimated 2.3 million households in the United States subscribed to cable modem services by the end of June 2000, with service available to an estimated 48 million households in North America (equal to 44% of all cable homes passed). Kinetic Strategies estimates, on average, more than 7000 new cable modem customers per day; it projects 15.9 installed cable modem customers in North America by the end of 2003.

According to the National Cable Television Association, cable operators will spend $33 billion before 2001 to upgrade their systems. The cable industry has been marked by a series of notable acquisitions and joint ventures during 1999. Of particular interest has been AT&T's purchase of cable giant Tele-Communications Incorporated (TCI) for $55 billion, as well as its planned $58 billion acquisition of MediaOne Group (pending regulatory approval). These acquisitions will make AT&T the largest cable company in the United States, with control of the leading cable Internet service providers (ISPs)—Excite@Home and Road Runner. AT&T has also concluded a deal with another cable company, Time Warner Cable, which would enable AT&T to offer telephone service over cable. Meanwhile, Microsoft is investing

$5 billion in a deal with AT&T to ensure access to the 2.5 to 5 million cable set-top boxes that AT&T plans to deploy (*ZDNET*, June 26, 1999).

Digital Subscriber Line, or DSL, is a modem technology which converts existing copper telephone lines into two-way high speed data conduits. While there are a number of types of DSL technologies, the most used currently is ADSL, or Asymmetric Digital Subscriber Line ("asymmetric" because transmission speed is higher from the Internet to the home than from the home to the Internet). ADSL is only available, at present, to homes within 18,000 feet (about three miles) of a central office facility.

According to TeleChoice Inc., 1.2 million DSL lines were in service in the United States by the end of June 2000. TeleChoice estimates that the number of U.S. DSL lines in service will grow to 2.1 million by the end of 2000, with further growth to 9.6 million DSL lines by the end of 2003. Telephone companies are currently rolling out DSL service in selected areas. Smaller telecommunications companies, that currently provide DSL service to businesses, are also seeking access to the residential DSL market. Additionally, a number of ISPs have signed cooperative arrangements with DSL providers.

Policy Issues

Section 706 of the Telecommunications Act of 1996 (P.L. 104-104) requires the FCC to determine whether "advanced telecommunications capability [i.e. broadband or high-speed access] is being deployed to all Americans in a reasonable and timely fashion." On January 28, 1999, the FCC adopted a report (FCC 99-5) pursuant to Section 706. The report concluded that "the consumer broadband market is in the early stages of development, and that, while it is too early to reach definitive conclusions, aggregate data suggests that broadband is being deployed in a reasonable and timely fashion." The FCC announced that it would continue to monitor closely the deployment of broadband capability in annual reports and that, where necessary, it would "not hesitate to reduce barriers to competition and infrastructure investment to ensure that market conditions are conducive to investment, innovation, and meeting the needs of all consumers."

The Commission's second Section 706 report was approved on August 3, 2000. Based on data collected from telecommunications service providers, an ongoing Federal-State Joint Conference to promote advanced broadband services, and the public, the report concluded that advanced telecommunications capability is being deployed in a reasonable and timely fashion overall, although certain groups of consumers were identified as being particularly vulnerable to not receiving service in a timely fashion. Those groups include rural, minority, low-income, and inner city consumers, as well as tribal areas and consumers in U.S. territories. The FCC acknowledges that more sophisticated data are still needed in order to portray a thoroughly accurate picture of broadband deployment.

While the FCC's position is not to intervene at this time, some assert that legislation is necessary to ensure fair competition and timely broadband deployment. Currently, the debate centers on three approaches. Those are: 1) compelling cable companies to provide "open access" to competing ISPs; 2) easing certain legal

restrictions and requirements (imposed by the Telecommunications Act of 1996) on incumbent telephone companies that provide high-speed data (broadband) access; and 3) providing federal financial assistance for broadband deployment in rural and economically disadvantaged areas. Hearings on broadband access have been held by a number of Congressional Committees, including House Commerce, House Judiciary, Senate Commerce, and Senate Judiciary. No action was taken on any these bills during the first session of the 106th Congress.

Open Access. Legislation introduced in the 106th Congress (H.R. 1685, Boucher; H.R. 1686, Goodlatte) would have the effect of requiring cable companies that provide broadband access to give "open access" to all Internet service providers. An additional measure, H.R. 2637 (Blumenauer), would enable ISPs to obtain access through leased commercial access provisions contained in Section 612 of the 1934 Communications Act. Currently, customers using cable broadband must sign up with an ISP affiliated or owned by their cable company. If customers want to access another ISP (such as America Online for example), they must pay extra—one monthly fee to the cable company's service (which includes the cable ISP) and another to their ISP of choice. In effect, the legislation would enable cable broadband customers to subscribe to their ISP of choice without first going through their cable provider's ISP. At issue is whether cable networks should be required to share their lines with, and give equal treatment to, rival ISPs who wish to sell their services to consumers. Supporters argue that open access is necessary to prevent cable companies from creating "closed networks," limiting access to content, and stifling competition. Opponents of open access counter that an open access mandate would inhibit the cable industry's ongoing nationwide investment in broadband technology, and assert that healthy competition does and will exist in the form of alternate broadband technologies such as DSL and satellites.

The arguments for and against open access are also being heard on the local level, as cities and counties begin to consider whether they will attempt to enforce open access requirements on local cable franchises. In June 1999, a federal judge ruled that the city of Portland, OR, had the right to require open access to the Tele-Communications Incorporated (TCI) broadband network as a condition for transferring its local cable television franchise to AT&T. AT&T appealed the ruling to the U.S. Court of Appeals for the Ninth Circuit. On June 22, 2000, the Court ruled in favor of AT&T, thereby reversing the earlier ruling. The court ruled that high-speed Internet access via a cable modem is defined as a "telecommunications service," which according to the Telecommunications Act of 1996, can be regulated only at the federal level (by the FCC). If the Court's decision stands, localities will be prevented from mandating open access on cable systems providing broadband access.

The debate thus moves to the federal level, where many interpret the Court's decision as giving the FCC authority to regulate broadband cable services as a "telecommunications service." However, the FCC also has the authority *not* to regulate if it determines that such action is unnecessary to prevent discrimination and protect consumers. To date, the FCC has chosen *not* to mandate open access, citing the infancy of cable broadband service and the current and future availability of competitive technologies such as DSL and satellite broadband services. However, in light of the June 22 court decision, the FCC announced, on June 30, 2000 that it will conduct a formal proceeding to determine whether or not cable-Internet service

should be regulated as a telecommunications service, and whether the FCC should mandate open access nationwide. According to FCC Chairman William Kennard, the FCC will begin collecting market information and creating a public record in order to formulate a decision.

Meanwhile, recent developments within the cable industry could have an impact on the open access debate. On December 6, 1999, AT&T announced an agreement to provide Mindspring (the nation's second largest ISP) access to its broadband cable system starting in mid-2002 (i.e. when AT&T's contract with its affiliated ISP, Excite@Home, expires). AT&T has pointed to the agreement with Mindspring as evidence that access issues should be left to market forces and need not be mandated by government regulation. While some critics see the AT&T-Mindspring agreement as a positive first step, others remain concerned that the agreement will not go into effect immediately, and worry that without government mandate, AT&T is not likely in the future to further provide other ISPs access to its broadband system.

On January 10, 2000, AOL announced plans to merge with Time Warner, Inc. If approved by the federal government, the merger would give AOL access to the second largest cable television system in the U.S., and a share in Roadrunner, one of the two major cable modem ISPs. Since the merger announcement, AOL has said it intends to open Time Warner's broadband cable platform to other ISPs. While still supporting the principle of open access, AOL has stated that it now prefers market solutions to a government mandate for open access. Subsequently, AOL has ceased lobbying for open access in states and local jurisdictions. Many supporters of open access have asserted that AOL's post-merger position, favoring market over government solutions, will ultimately leave many of the nation's 6000 ISPs without broadband access. However, on February 29, 2000, AOL and Time Warner took a further step toward open access by signing a memorandum of understanding (MOU) that commits the company to provide access to as many ISPs as is technically possible. The MOU pledges no restrictions on video streaming, no discrimination based on affiliation, and no restrictions on ISP direct billing and collections. Specific details of the proposal are not yet available.

Easing Restrictions and Requirements on Incumbent Telephone Companies. Legislative proposals (H.R. 1685, Boucher; H.R. 1686, Goodlatte; H.R. 2420, Tauzin; S. 877, Brownback; and S. 1043, McCain) would ease certain legal restrictions and requirements imposed by the Telecommunications Act of 1996 on ILECs (incumbent local exchange companies such as Bell Atlantic, US West, or GTE). Included among the proposed legislative remedies are allowing Bell operating companies (BOCs) to offer data services across local access and transport area

(LATA) boundaries,[10] and easing requirements for ILECs to share (via unbundling and resale) their high speed networks with competing companies.[11]

Those supporting these provisions, primarily the BOCs, claim they are needed to promote the deployment of broadband services, particularly in rural and under served areas. Present regulations contained in the 1996 Telecommunications Act, they claim, are overly burdensome and discourage needed investment in broadband services. ILECs, they state, are the only entities likely to provide such services in low volume rural and other under served areas. Therefore, proponents state, until present regulations are removed the development and the pace of deployment of broadband technology and services, particularly in unserved areas, will be lacking. Furthermore, supporters state, domination of the Internet backbone[12] market is emerging as a concern and entrance by ILECs (particularly the BOCs) into this market will ensure that competition will thrive with no single or small group of providers dominating. Additional concerns that the lifting of restrictions on data would remove BOC incentives to open up the local loop to gain interLATA relief for voice services are also unfounded, they state. The demand by consumers for bundled services and the large and lucrative nature of the long distance voice market will, according to proponents, provide the necessary incentives for BOCs to seek relief for interLATA voice services.

Opponents, including long distance companies and non-incumbent local exchange companies (those competing with the ILECs to provide local service), claim that lifting such restrictions and requirements will undermine the incentives needed to ensure that the ILECs will open up their networks to competition. Present restrictions, opponents claim, were built into the 1996 Telecommunications Act to help ensure that competition will develop in the provision of telecommunications services. Modification of these regulations, critics claim, will remove the incentives

---

[10]As a result of the 1984 AT&T divestiture, the Bell System service territory was broken up into service regions and assigned to a regional Bell operating company (BOC). The geographic area in which a BOC may provide telephone services within its region was further divided into local access and transport areas, or LATAs. Telephone traffic that crosses LATA boundaries is referred to as interLATA traffic. Present restrictions contained in Section 271 of the Telecommunications Act of 1996 prohibit the BOCs from offering interLATA services within their service regions until certain conditions are met. To date one BOC, Bell Atlantic, has received approval to enter the in-region interLATA market in New York state; Bell Atlantic began to offer in-region long distance service to its New York state customers effective January 5, 2000. Another BOC, SBC Communications, has filed an application with the FCC seeking approval to offer in-region interLATA services in Texas; that application is still pending.

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

[12]An Internet backbone is a very high speed, high capacity data conduit that local or regional networks connect to for long-distance interconnection.

needed to open up the "monopoly" in the provision of local services. Competitive safeguards such as unbundling and resale are necessary, opponents claim, to ensure that competitors will have access to the "monopoly bottleneck" last mile to the customer. Therefore they state, the enactment of this legislation to modify these regulations will all but stop the growth of competition in the provision of local telephone service. A major change in existing regulations, opponents claim, would not only remove the incentives needed to open up the local loop but would likely result in the financial ruin of providers attempting to offer competition to the ILECs. As a result, consumers will be hurt, critics claim, since the hoped for benefits of competition such as increased consumer choice and lower rates will never emerge. Concern over the inability of regulators to distinguish between the provision of voice only and data services if such restrictions are lifted has also been expressed. Opponents also dismiss arguments that BOC entrance into the marketplace is needed to ensure competition. The marketplace, opponents claim, is a dynamic and growing one, and concerns over the lack of competition and market dominance are misplaced.

Federal Assistance for Broadband Deployment. Broadband issues will likely be considered during the FY2001 appropriations process, as Congress reviews and considers the Administration's proposed "digital divide" initiative. As part of that initiative, the Administration is requesting $25 million in grants and loan guarantees to accelerate private sector deployment of broadband networks in under-served urban and rural communities. The FY2001 request includes $23 million for the Economic Development Administration's (Dept. of Commerce) new e-commerce initiative, and $2 million for a pilot grant program in the Distance Learning and Telemedicine Program of the Rural Utilities Service (U.S. Dept. of Agriculture). Additionally the Administration is requesting $2 million for broadband technology research and standards development at the National Telecommunications and Information Administration, Department of Commerce.

Congress has also begun to consider legislation that would provide financial support for broadband deployment, especially in rural areas. In response to a request by ten Senators, the Departments of Commerce and Agriculture released a report on April 26, 2000, concluding that rural areas lag behind urban areas in access to broadband technology. The report found that less than 5% of towns of 10,000 or less have access to broadband. In response to concerns over rural and low-income area broadband deployment, a number of bills have been introduced into the 106th Congress which seek to provide assistance for broadband deployment through mechanisms such as: tax credits for investment in broadband facilities, support from the FCC's universal service fund, and loans from the Rural Utilities Service (RUS) of the Department of Agriculture.

106th Congress Legislation

Encryption

H.R. 850, Goodlatte, Safety and Freedom Through Encryption Act (Judiciary, International Relations, Armed Services, Commerce, Intelligence)
H.R. 2616, Goss, Encryption for the National Interest (Judiciary, International Relations, Government Reform)
H.R. 2617, Goss, Tax Relief for Responsible Encryption (Ways and Means)

S. 798, McCain, Promote Reliable On-Line Transactions to Encourage Commerce and Trade Act (Commerce)

Electronic/Digital Signatures

H.R. 439, Talent, Paperwork Elimination Act of 1999 (passed House, referred to Senate Governmental Affairs)
H.R. 1320, Eshoo, Millennium Digital Commerce Act (Commerce, Government Reform)
H.R. 1685, Boucher, Internet Growth and Development Act of 1999 (Commerce, Judiciary)
H.R. 1714, Bliley, Electronic Signatures in Global and National Commerce Act (Commerce)
H.R. 1572, Gordon, Digital Signature Act (Science)
H.R. 2413, Sensenbrenner, Computer Security Enhancement Act of 1999 (Science)

S. 761, Abraham, Millennium Digital Commerce Act (Commerce)
S. 921, Abraham, Electronic Securities Transactions Act (Banking)

Computer Security

H.R. 2162, Miller, Can Spam Act (Commerce, Judiciary)
H.R. 2413, Sensenbrenner, Computer Security Act of 1999 (Science)
H.R. 2816, Salmon, Computer Crime Enforcement Act (Judiciary)
H.R. 4210, Fowler, Preparedness Against Terrorism Act of 2000 (Transportation)
H.R. 4246, Davis, Cyber Security Information Act (Government Reform, Judiciary)
H.R. 4347, Andrews, A bill to amend Title 18 and other purposes (Judiciary, Armed Services)
H.R. 5024, Davis, Federal Information Policy Act of 2000, (Government Reform)

S. 1314, Leahy, Computer Crime Enforcement Act (Judiciary)
S. 1993, Thompson, Government Information Security Enhancement Act of 1999 (Government Affairs)
S. 2092, Schumer, A bill to amend Title 18... (Judiciary)
S. 2430, Leahy, Internet Security Act of 2000 (Judiciary)
S. 2451, Hutchison, A bill to increase criminal penalties for computer crimes... (Judiciary)
S. 2448, Hatch, Internet Integrity and Critical Infrastructure Protection Act of 2000

(Judiciary)
S. 2545, Roberts, Barry Goldwater Scholarship and Excellence in Education Enhancement Act (Health)

Internet Privacy

H.R. 313, Vento, Consumer Internet Privacy Protection (Commerce)
H.R. 367, Franks, Social Security On-line Privacy Act (Commerce)
H.R. 369, Franks, Children's Privacy Protection and Parental Empowerment Act (Judiciary)
H.R. 1685, Boucher, Internet Growth and Development Act (Commerce, Judiciary)
H.R. 2882, Vento, Internet Consumer Information Protection Act (Commerce)
H.R. 3221, Markey, Electronic Privacy Bill of Rights (Agriculture, Banking, Commerce, Transportation)
H.R. 3560, Frelinghuysen, Online Privacy Protection Act (Commerce)
H.R. 3770, Jackson, Secure Online Communications Enforcement Act (Judiciary)
H.R. 4049, Hutchinson-Moran, Privacy Commission (Government Reform)
H.R. 4311, Hooley, Identify Theft Prevention Act (Banking)
H.R. 4611, Markey, Social Security Number Protection Act (Commerce, Ways and Means)
H.R. 4857, Shaw, Privacy and Identity Protection Act (Ways and Means, Judiciary, Banking, and Commerce)
H.R. 4690, Rogers, FY2001 Commerce, Justice, State Appropriations (Appropriations)
H.R. 4871, Kolbe, FY2001 Treasury-Postal Appropriations (Appropriations)
H.R. 4987, Barr, Digital Privacy Act of 2000, 7/27/00 (Judiciary)

S. 809, Burns, Online Privacy Protection Act (Commerce)
S. 854, Leahy, Electronic Rights for the 21st Century (Judiciary)
S. 2063, Torricelli, Secure Online Communication Enforcement Act (Judiciary)
S. 2328, Feinstein, Identity Theft Protection Act (Banking)
S. 2448, Hatch, Internet Integrity and Critical Infrastructure Protection Act (Judiciary)
S. 2554, Gregg, Amy Boyer's Law (Finance)
S. 2699, Feinstein, Social Security Number Protection Act (Finance)
S. 2857, Leahy, Privacy Policy Enforcement in Bankruptcy Act (Judiciary)
S. 2871, Shelby, Social Security Number Privacy Act (Banking)
S. 2876, Bunning, Privacy and Identity Protection Act (Finance)
S. 2924, Collins, Internet False Identification Prevention Act (Judiciary)
S. 2928, McCain, Consumer Internet Privacy Enhancement Act (Commerce)

Protecting Children

Filtering

H.R. 368, Franks, Safe Schools Internet Act (Commerce)
H.R. 543, Franks, Children's Internet Protection Act (Commerce)
H.R. 896, Franks, Children's Internet Protection Act (Commerce)
H.R. 1501, McCollum, Juvenile Justice bill (Judiciary)

H.R. 2560, Istook, Child Protection Act (Education)
H.R. 4141, Goodling, Education Opportunities To Protect and Invest In Our Nation's Students (Education OPTIONS) Act (Education)
H.R. 4577, Porter, FY2001 Labor-HHS-Education Appropriations Bill (Appropriations)
H.R. 4600, Pickering, Children's Internet Protection Act, 6/8/00 (Commerce)

S. 97, McCain, Child Internet Protection Act (Commerce)
S. 254, Hatch, Juvenile Justice Bill (Judiciary)
S. 1545, Santorum, Neighborhood Children's Internet Protection Act (Commerce)

Protecting Against Predators on the Internet

H.R. 640, Lampson, to authorize appropriations for cybersmuggling (Ways and Means)
H.R. 1159, Johnson, Protection of Children from On-Line Predators and Exploitation Act (Ways and Means, Judiciary)

Fraud

H.R. 612, Weygand, Protection Against Scams on Seniors (Commerce, Judiciary)
H.R. 4311, Hooley, To prevent identity fraud in consumer credit transactions and credit reports (Banking)

S. 699, Wyden, Telemarketing Fraud and Seniors Protection Act (Judiciary)
S. 1015, Schumer, Online Investor Protection Act (Banking)

Spam

H.R. 1685, Boucher, Internet Growth and Development Act (Commerce, Judiciary)
H.R. 1686, Goodlatte, Internet Freedom Act (Judiciary, Commerce)
H.R. 1910, G. Green, E-Mail User Protection Act (Commerce, Judiciary)
H.R. 2162, G. Miller, Can Spam Act (Commerce, Judiciary)
H.R. 3024, C. Smith, Netizens Protection Act (Commerce)
H.R. 3113, Wilson, Unsolicited Electronic Mail Act (passed House, referred to Senate Commerce Committee)

S. 759, Murkowski, Inbox Privacy Act (Commerce)
S. 2448, Hatch, Internet Integrity and Critical Infrastructure Protection Act (Judiciary)
S. 2542, Burns, Controlling the Assault of Non-Solicited Pornography and Marketing Act (Commerce)

Internet Domain Names

H.R. 749, Terry, Home Page Tax Repeal Act (Science, Ways and Means)
H.R. 2797, Terry, Home Page Tax Repeal Act (Science, Ways and Means)
H.R. 3028, Rogan, Trademark Cyberpiracy Prevention Act (Judiciary)

S. 705, Ashcroft, Home Page Tax Repeal Act (Commerce)
S. 1255, Abraham, Anticybersquatting Consumer Protection Act (Judiciary)
S. 1461, Hatch, Domain Name Piracy Prevention Act of 1999 (Judiciary)

Broadband Internet Access

H.R. 1685, Boucher, Internet Growth and Development Act of 1999 (Commerce, Judiciary)
H.R. 1686, Goodlatte, Internet Freedom Act (Judiciary, Commerce)
H.R. 2420, Tauzin, Internet Freedom and Broadband Deployment Act of 1999 (Commerce).
H.R. 2637, Blumenauer, Consumer and Community Choice in Access Act of 1999 (Commerce)
H.R. 4122, Stupak, Rural Broadband Enhancement Act (Commerce, Agriculture)
H.R. 4477, Towns, Digital Bridge Trust Fund Act (Commerce, Ways and Means, Education, Transportation, Banking)
H.R. 4728, English, Broadband Internet Access Act (Ways and Means)
H.R. 5069, Minge, Comprehensive Rural Telecommunications Act (Commerce, Ways and Means, Agriculture)

S. 877, Brownback, Broadband Internet Regulatory Relief Act of 1999 (Commerce)
S. 1043, McCain, Internet Regulatory Freedom Act of 1999 (Commerce)
S. 2307, Dorgan, Rural Broadband Enhancement Act (Commerce)
S. 2321, Rockefeller, Rural Telecommunications Modernization Act (Commerce)
S. 2097, Burns, Launching Our Communities' Access to Local Television Act of 2000 (Banking)
S. 2454, Burns, authorizes low-power television stations to provide digital data services including high-speed Internet access (Commerce)
S. 2698, Moynihan, Broadband Internet Access Act (Finance)

Related CRS Reports

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

Computer Fraud & Abuse: A Sketch of 18 U.S.C. 1030 And Related Federal Criminal Laws, by Charles Doyle. CRS Report 97-1024 A. 5 p. December 3, 1997.

Computer Fraud & Abuse: An Overview of 18 U.S.C. 1030 And Related Federal Criminal Laws, by Charles Doyle. CRS Report 97-1025 A. 85 p. November 28, 1997.

Critical Infrastructures: Background and Early Implementation of PDD-63, by John D. Moteff. CRS Report RL30153, 21 p. March 8, 2000.

Digital Millennium Copyright Act: P.L. 105-304: Summary and Analysis, by Dorothy Schrader. CRS Report 98-943 A. 23 p. November 10, 1998.

Electronic Commerce: An Introduction, by Glenn J. McLoughlin. CRS Report RS20426. 6 p. June 27, 2000.

Electronic Commerce, Info Pack. by Rita Tehan. IP539P (Updated as needed)

Electronic Stock Market, by Mark Jickling. CRS Report RL30602. 15 p. July 8, 2000.

Electronic Signatures: Technology Developments and Legislative Issues, by Richard Nunno. CRS Report RS20344. 6 p. July 13, 2000.

Encryption Debate: Intelligence Aspects, by Richard A. Best and Keith G. Tidball. CRS Report 98-905 F. 6 p. November 4, 1998.

Encryption Export Controls, by Jeanne J. Grimmett. 23 p. CRS Report RL30273. May 10, 2000.

Encryption Technology: Congressional Issues, by Richard Nunno. CRS Issue Brief IB96039. (Updated Regularly)

Intellectual Property Protection for Noncreative Databases, by Dorothy Schrader and Robin Jeweler. CRS Report 98-902 A. 17 p. September 15, 1999.

Internet and E-Commerce Statistics: What They Mean and Where to Find Them on the Web, by Rita Tehan. CRS Report RL30435. 12 p. February 17, 2000.

Internet Domain Names: Background and Policy Issues, by Lennard G. Kruger. CRS Report 97-868 STM. 6 p. June 1, 2000.

Internet Gambling: A Sketch of Legislative Proposals, by Charles Doyle. CRS Report RS20485. 6 p. July 26, 2000.

Internet Gambling: Overview of Federal Criminal Law, by Charles Doyle. CRS Report 97-619 A. 43 p. March 7, 2000.

Internet Privacy—Protecting Personal Information: Overview and Pending Legislation, by Marcia S. Smith. CRS Report RS20035. 6 p. August 24, 2000.

Internet—Protecting Children from Unsuitable Material and Sexual Predators: Overview and Pending Legislation, by Marcia S. Smith. CRS Report RS20036. 6 p. August 22, 2000.

Internet Service and Access Charges, by Angele Gilroy. CRS Report RS20579. 3 p. May 12, 2000.

Internet Taxation: Bills in the 106th Congress, by Nonna Noto. CRS Report RL30412. 23 p. July 6, 2000.

Internet Transactions and the Sale Tax, by Stephen Maguire. CRS Report RL30431. 11 p. July 13, 2000.

Internet Voting: Issues and Legislation, by Kevin Coleman and Richard Nunno. CRS Report RS20639. 6 p. August 1, 2000.

"Junk E-mail": An Overview of Issues and Legislation Concerning Unsolicited Commercial Electronic Mail ("Spam"), by Marcia S. Smith. CRS Report RS20037. 6 p. July 20, 2000.

Legislation to Prevent Cybersquatting/Cyberpiracy, by Henry Cohen. CRS Report RS20367. 5 p. May 1, 2000.

Medical Records Confidentiality, C Stephen Redhead, Harold C. Relyea, and Gina M. Stevens. CRS Issue Brief IB98002. (Updated Regularly)

National Information Infrastructure: The Federal Role, by Glenn J. McLoughlin. CRS Issue Brief 95051. (Updated Regularly)

Noncreative Database Bills in the House, by Robin Jeweler. CRS Report RS20361. 6 p. October 19, 1999.

Obscenity, Child Pornography, and Indecency: Recent Developments and Pending Issues, by Henry Cohen. CRS Report 98-670 A. 6 p. June 27, 2000.

Prescription Drug Sales Over the Internet, by Christopher Sroka. CRS Report RL30456. 8 p. March 10, 2000.

Recent Developments in Copyright Case Law: Napster and MP3 Digital Music, by Robin Jeweler. CRS Report RS20610. 6 p. August 9, 2000.

Spinning the Web: the History and Infrastructure of the Internet, by Rita Tehan. CRS Report 98-649 C. 16 p. August 12, 1999.

State Sales Taxation of Internet Transactions, by John Luckey. CRS Report RS20577. 3 p. May 7, 2000.

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

Telemarketing Fraud: Congressional Efforts to Protect Consumers, by Bruce Mulock. CRS Report 98-514 E. 6 p. June 2, 1998.

World Intellectual Property Organization Copyright Treaty: An Overview, by Dorothy Schrader. CRS Report 97-444 A. 27 p. September 10, 1998.

World Intellectual Property Organization Performance and Phonograms Treaty: An Overview, by Dorothy Schrader. CRS Report 97-523. 35 p. September 10, 1998.

Document No. 178