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

Updated August 21, 1998

Marcia S. Smith
Jane Bortnick Griffith
Richard M. Nunno
John D. Moteff
Science, Technology, and Medicine Division

ABSTRACT

This report summarizes six key issues that could affect the growth and use of the Internet from a technology policy perspective: encryption and digital signatures; computer security; computer privacy (including consumer identity theft, protecting children from unsuitable material, and privacy of information in government databases), intellectual property rights, unsolicited electronic mail ("junk e-mail" or "spamming"), and Internet domain names. Identification of related legislation and other CRS reports that provide more detail on the issues is included. This report will be updated if necessary.

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

Summary

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

1. The use of cryptography to protect the privacy of communications (encryption) and to authenticate and verify the origin and content of messages (digital signatures). To date, Congress has focused on the encryption debate, which concerns balancing the interests of personal privacy, competitiveness of U.S. computer companies, and law enforcement and national security requirements. However, digital signature issues are beginning to receive attention, too, particularly the respective roles of federal versus state laws governing their use.

2. Concerns about computer security, particularly unauthorized access or "hacking," are prevalent both in government and the private sector. Congress already has passed laws imposing penalties for hacking into many types of computers (18 U.S.C. 1030), but hacking continues to be a problem. Issues also have been raised about the vulnerability of the nation's critical infrastructure (e.g., electrical power grids and telecommunications) to cyber attacks.

3. Individuals and businesses considering whether to use the Internet are increasingly concerned about issues such as computer fraud and scams, consumer identity theft (where one person assumes the identify of another by using credit card or Social Security numbers, for example), protecting children from unsuitable material, and the privacy of information stored in computer databases.

4. Protection of intellectual property rights presents significant challenges as exact duplicates of material are created and transmitted by computer. Copyright holders want to protect their rights, while some organizations and institutions (particulary academia and scientific researchers) want to make certain they are not denied access to material traditionally available under the "fair use" principle.

5. An unwelcome aspect of the computer age is unsolicited electronic mail or "junk e-mail" ("spamming"). Not only is it a nuisance, but the cost may be passed on to the consumer through higher charges from Internet service providers who must upgrade their systems to handle the traffic. Another concern is some junk e-mail contains pornographic material or links to pornographic Web sites.

6. Navigating the Internet requires using addresses that identify the location of individual computers. How to allocate and designate these "domain names" has become controversial. Among the issues is what role the government should play in governing the domain name system, approaches to resolving trademark disputes, how to foster competition in registration services, and the disposition of monies collected from registration fees for infrastructure improvements.

Contents

Internet: An Overview of Six Key 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 pending before Congress. Among them are ensuring the privacy of information transmitted over the Internet or stored in computer databases, establishing "trustworthiness" by authenticating and verifying the origin and content of messages, protecting children from unsuitable material, safeguarding system security, protecting intellectual property, limiting unsolicited electronic mail, and issuing Internet domain names. 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 for each issue, and a list of the bills by topic is provided at the end.

Cryptography: Encryption and Digital Signatures

Cryptography can be used to ensure the confidentiality of data and messages (encryption), as well as to authenticate the sender of a computer message and to verify that nothing in the message has been changed (digital signatures).

Encryption

Encryption and decryption are methods of applying the science of cryptography to ensure the privacy of data and communications. CRS Issue Brief 96039, *Encryption Technology: Congressional Issues*, discusses the topic in more detail.

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.

The Clinton Administration supports the wide use of strong encryption as long as it has 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 has raised privacy issues. Also, although there currently are no limits on what type of encryption is sold in or imported into the United States, the Administration has sought to influence what type of products are available domestically by limiting exports, knowing that companies do not want to make one product for domestic use and another for export. This has raised industry concerns about placing U.S. computer hardware and software companies at a competitive disadvantage because they are subject to restraints on what they can export. The congressional debate today over encryption policy is focused on striking a "balance" among individual rights of privacy; the global competitiveness of U.S. companies making, using, or selling encryption products; promotion of secure electronic commerce; and law enforcement and national security needs to monitor undesirable behavior.

In 1996, the Clinton Administration developed new 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. Until December 1996, only 40 bit encryption could be easily exported. Under the new regulations, released on December 30, 1996, for two years companies can easily export 56 bit encryption products if they agree to incorporate key recovery features into the product within those two years. If they already have incorporated key recovery into the product, there is no limit on the bit length that can be exported. (Some exceptions are made for banking.) The Administration is now reviewing what should happen at the end of 1998 when the provisions regarding 56 bit exports are due to expire.

Four bills in the Senate (S.376, Leahy; S.377, Burns; S.909, McCain; and S.2067, Ashcroft) and three in the House (H.R.695, Goodlatte; H.R.1964, Markey; and H.R.1903, Sensenbrenner, which passed the House in September) address these issues. CRS Issue Brief 93069 provides further information on the content and status of the bills.

Six of the seven bills (all except H.R.1964) address the export issue. In summary, H.R.695 (Goodlatte, as introduced), S.376 (Leahy), and S.377 (Burns), seek to relax export controls on encryption, although versions of H.R.695 as reported from various committees have substantially different provisions. S.909 (McCain) would permit easy export of 56 bit encryption without key recovery, and easy export of any strength encryption if it is based on a qualified system of key recovery. (S.909 further provides that the 56 bit limit can increase as recommended by an Encryption Export Advisory Board established by the Act unless the President determines it would harm national security. The bill also allows the President to waive any provision of the bill, including the export limits, in the interest of national security, or domestic safety and security.) Modifications to S.909 announced by Senators McCain and Kerrey on March 4, 1998 include allowing U.S. companies to export products with optional recovery features to approved end users. S.2067 would allow the removal of controls for encryption products that are deemed to be generally available in the international market, and would allow 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 primary section of H.R.1903 (Sensenbrenner) that dealt with export issues (section 7) was deleted before it passed the House, but the bill still calls for export policy to be determined in light of the "public availability of comparable technology."

In the key recovery concept, a "key recovery agent" (or "key holder" in S. 376) would hold a copy of the decryption key. (Or 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 questions involve 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. The Administration's December 30, 1996 regulations establish criteria for key recovery agents that the Department of Commerce uses to support its decisions on whether or not to approve the export of key recovery encryption products. In addition, the Administration has sought legislation to provide liability protection for such agents, as well as penalties if they make an unauthorized release of such information. S.376 (Leahy) and S.909 (McCain) both address those issues.

Another element needed for the widespread use of encryption is certificate authorities who would 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. The combination of public key encryption and certificate authorities (some would add key recovery agents) is referred to as a "public key infrastructure" (PKI). There is debate over whether there should be a single, global PKI, or many different PKIs, but the establishment of one or more PKIs is expected to add the requisite element of "trust" to the Internet needed for its use

to expand. H.R.1903 (Sensenbrenner) calls for a National Research Council study of PKIs.

Originally, S.909 established mechanisms for the government to register key recovery agents and certificate authorities. While registration would have been voluntary, they would not have been fully covered by the bill's liability protections if they did not register. If a certificate authority registered with the government, it could only issue certificates to persons who had stored key recovery information with a government-registered key recovery agent or made other arrangements to assure lawful recovery of plaintext in a timely fashion. The linkage between certificate authorities and key recovery was controversial because some observers felt that the ability to issue certificates should be independent from the debate over key recovery. In March 1998, Senators McCain and Kerrey announced modifications to S. 909 including deletion of that linkage. H.R.1964 (Markey) and H.R.695 as reported from the House Commerce Committee prohibit conditioning the issuance of certificates on escrowing or sharing of encryption keys.

The Clinton Administration repeatedly has indicated that it will not seek to change current 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 now become an integral part of the encryption debate. Hence, many find the Administration's position unclear. Publicly, it maintains that it is not proposing domestic use restraints, but it has not prevented the FBI Director from promoting that course of action. Civil liberties groups in particular are opposed to domestic use controls. S.376 (Leahy), S.909 (McCain), and S.2067 (Ashcroft) all prohibit mandatory key recovery and provide that persons in any state (and U.S. persons in foreign countries per S.376 and S.2067) may use any type of encryption they choose except as otherwise provided by the Act. S.377 (Burns), H.R.695 (Goodlatte, as introduced), and H.R.1964 (Markey) say that federal and state governments may not restrict or regulate the sale of encryption products solely because they have encryption. The House Intelligence Committee's version of H.R. 695 includes provisions supportive of the FBI's position. A similar amendment was defeated by the House Commerce Committee during its markup of the bill.

On March 4, 1998, Vice President Gore wrote to Senator Daschle restating the Administration's desire for a "balanced approach" to encryption policy and seeking a "good faith dialogue" to "produce cooperative solutions, rather than seeking to legislate domestic controls." The letter added that the discussions could also enable additional steps to relax export controls on encryption products. On April 15, Secretary of Commerce Daley made a speech wherein he said that although the Administration's policy was the right one, its implementation was a failure. He urged both industry and government to strive harder to reach consensus on the issue. At an April 24, 1998 meeting of the Congressional Internet Caucus, Undersecretary of Commerce William Reinsch commented that the Administration is not seeking a legislative solution to encryption issues this year. Representative Goodlatte and

Senators McCain and Kerrey have each expressed optimism that their respective bills will come to the floor for debate this year, however.

There have been several recent developments. On July 7 the Administration announced plans to relax export controls for strong encryption without key recovery for financial institutions in countries with acceptable money laundering laws. Additionally, a group of software companies announced on July 13 their plans to develop a product to capture data before it is encrypted and sent over the Internet that could be given to law enforcement. While that proposal might generate more business for companies offering encryption products, it does nothing to satisfy the demands of advocates of electronic privacy.

Digital Signatures

Another use of cryptography on the Internet is for authentication and verification. Digital signatures, which are unique to each individual and to each message, 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 valid signatures can be produced for use in electronic commerce. Digital signatures typically encrypt only the identification information and not the content of a message. (Digital signatures are one type of electronic signature. In general, electronic signatures can refer to any electronically created identifier meant to authenticate a writing, but do not necessarily involve encryption.)

While neither law enforcement nor national security organizations oppose the use of digital signatures, many question whether a standard for digital signatures should be established to enhance electronic commerce. Of a total of 40 states that have enacted or are considering electronic signature laws, 10 have enacted digital signature or combination electronic/digital signature laws (Florida, Indiana, Minnesota, Mississippi, New Hampshire, New Mexico, Oregon, Utah, Virginia, and Washington). Another eight are considering them. These laws are summarized in *Survey of State Electronic & Digital Signature Legislative Initiatives* by Albert Gidari and John Morgan of Perkins Cole. The article is available on the Internet Law & Policy Forum's (ILPF's) Web site:[http:// www.ilpf.org/digdig/digrep.htm]. Links to the texts of the state laws are provided on another ILPF Web site, www.ilpf.org/digsig/digsig2.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 digital signatures is whether there should be a single federal law in place of the various state laws.

Two bills are pending in the House and two in the Senate regarding digital signatures — H.R.2937 (Baker), H.R.2991 (Eshoo), S.1594 (Bennett), and S.2107 (Abraham). Also, the House passed H.R.1903, the Computer Security Enhancement Act, on September 16 which includes a provision establishing a panel to develop policy, guidelines, and technical standards for digital signatures. The House Banking Committee held a hearing on the federal role in electronic authentication on July 9, 1997. The House Science Committee held a hearing on digital signatures on October 28, 1997. The Senate Banking Committee held a general hearing on the topic on October 28, 1997 and specifically on S.1594 on March 11, 1998. The Senate Commerce Committee held a hearing on S.2107 on July 15, 1998.

Computer Security

Unauthorized access to computer networks ("hacking," or colloquially, "cracking") is 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. Some of the best data publicly available so far are contained in 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). 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. In 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 have not been publicly acknowledged, however.

A 1998 survey by the Computer Security Institute (CSI) conducted in cooperation with the FBI concluded that computer crime and computer security breaches increased 16% over its 1997 survey. Those breaches include more than just "hacking" incidents, however, and include theft of proprietary information, sabotage, insider abuse of Internet access, financial fraud, spoofing, denial of service, viruses, telecommunications fraud, wiretapping, eavesdropping, and laptop theft. Losses ranged from $50 due to a computer virus to $50 million for unauthorized insider access. Unauthorized access can be attributed either to insiders or outsiders. CSI reported that losses from unauthorized insider access ranged from $1,000 to the $50,000,000 previously noted, with an average of $2,809,000. For unauthorized outsider access ("system penetration by outsider"), losses ranged from $500 to $500,000, with an average loss of $86,000. Total losses in 1998 from all categories of computer crime and computer security breaches was listed as $136,822,000. Tables from the CSI report and a press release are available at [http://www.gosci.com/prelea11.htm]. The Joint Economic Committee held a hearing on "Cybercrime, Transnational Crime and Intellectual Property Theft" on March 24, 1998 highlighting the FBI's role in fighting such crime.

Of particular concern recently 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.

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 is being set up in the Department of Commerce to help coordinate the development of these plans. A Critical Infrastructure Coordination Group, an interagency group that will address interdependencies between agencies and sectors, chaired by a National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, and will report 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 Investigations to be the executive agent for a National Infrastructure Protection Center (NIPC). While run by the FBI, the NIPC will include representatives from the Department of Defense, the Intelligence Community, and the lead agencies. The NIPC will be the operational focal point for coordinating federal response to "attacks", drawing upon expertise found throughout the federal government. The NIPC will also be the federal point of contact for developing threat analyses, issuing warnings and sharing information regarding intrusions, hacking methods and fixes. The PDD encourages the private sector to set up a parallel center to interact with the NIPC.

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 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.

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.

Computer Privacy

Computer Fraud and Scams, Protection of Personal Information, and General Computer Privacy Issues

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. The Senate Governmental Affairs Committee's Permanent Subcommittee on Investigations held a hearing on the topic on February 10, 1998. On July 14, 1998, the Federal Trade Commission (FTC) released a list of the 12 most common scams found in unsolicited commercial electronic mail (for a general discussion of unsolicited email, see below). The list is available on the World Wide Web at [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.

As noted above, 18 U.S.C. 1030 addresses computer fraud, and the United States and seven other countries agreed in December 1997 to coordinate their efforts at fighting computer crime, including fraud. On May 12, 1998, just prior to President Clinton's attendance at the G-8 meeting, the White House announced an International Crime Control Strategy (ICCS) and proposed related legislation (S. 2303, Leahy) to provide new authorities and resources to fight international crime including fraud involving credit cards and other access devices, and authorizing wiretapping for investigations of felony computer crime offenses.

Consumer identity theft, in which one individual assumes the identity of another using personal information such as credit card and Social Security numbers, is also seen as increasing due to the widespread use of computers for storing and transmitting information. Congress directed the Federal Reserve Board to study the issue of the availability to the public of sensitive identifying information, whether such information could be used to commit financial fraud, and the risk to insured depository institutions. Its March 1997 report, *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. A May 1998 General Accounting Office report, *Identity 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.

Many bills have been introduced in the Senate and House regarding protection of personally identifiable information generally, and specifically Social Security numbers. Some of the legislation is targeted towards all consumers, while other bills focus primarily on preventing acquisition of a child's personally identifiable information without a parent's knowledge, or attempting to obtain information about parents from children. The major provisions of many of those bills are summarized in CRS Report 97-1061, *Protecting Privacy on the Internet: A Summary of Legislative Proposals*. CRS Report 97-833, *Information Privacy*, provides more information on the legal aspects of these issues.

In summary, the Senate has passed one bill (S. 512) and three others are pending (S. 504, Feinstein; S. 600, Feinstein, and S. 2326, Bryan). S. 512 was reported from the Senate Judiciary Committee on July 9 without written report and passed the Senate on July 30, 1998. The bill 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. Vice President Gore hailed the passage of this bill in his July 31 press conference (see below).

Twelve bills are pending in the House (H.R. 98, Vento; H.R. 1287, Franks; H.R. 1330, Kanjorski; H.R. 1331, Kennelly; H.R. 1367, Barrett; H.R. 1813, Kleczka; H.R. 1964, Markey; H.R. 1972, Franks; H.R. 2368, Tauzin; H.R. 3551, DeLauro; H.R. 3601, Shadegg; and H.R. 4151, Shadegg). The House Judiciary Subcommittee on Courts and Intellectual Property held a general hearing on privacy in electronic communications on March 26, 1998. That Committee's Subcommittee on Crime held a hearing on H.R. 1972 and related legislation on April 30, 1998.

The House Commerce Committee's Subcommittee on Telecommunications held a hearing on H.R. 2368 on July 21, 1998. The bill would provide incentives to industry to develop and implement voluntary privacy guidelines. The hearing focused on efforts to encourage the private sector to self regulate in this area.

Voluntary self regulation also has been the focus of the Clinton Administration's approach to Internet privacy. In its July 1997 report, *A Framework for Global Electronic Commerce,* the Administration endorsed industry self regulation for protecting consumer Internet privacy, stressing that if industry did not self-regulate effectively, the government might have to step in, particularly regarding children's Internet privacy.

The Federal Trade Commission held a public workshop in June 1996 that addressed general issues of online privacy. Another workshop, in June 1997, 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 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 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.

On July 16, 1997, the FTC issued a letter advising the online industry that it was a deceptive practice to collect personal information from children without fully disclosing to parents how the data would be used and that Web sites must obtain parental permission before releasing such data to third parties. In December 1997, the FTC conducted a survey of 126 children's Web sites to determine the extent to which information collection practices were being disclosed. It found 86% of the Web sites collected information from children but fewer than 30% posted a privacy policy statement and only 4% required parental notification. Another survey was conducted in June 1998 of a broader range of 1,400 Web sites intended for children or adults. In its subsequent report, *Privacy Online: A Report to Congress* [http://www.ftc.gov/reports/privacy3/index.htm], the FTC reported that of the 212 children's sites in this survey, 89% collected personal identifiable information but only 54% disclosed their information collection practices and fewer than 10% provided any form of parental control. The survey also included 674 commercial Web sites of which 92% collected personal information. Only 14% provided any notice of their information collection practices and only 2% provided a comprehensive privacy policy.

Frustrated at those 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. Vice President Gore issued a statement supporting the FTC's actions. At a June 23-24, 1998 "summit" on Internet privacy organized by the Department of Commerce at the direction of the White House, 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. At the July 21 House Commerce Telecommunications Subcommittee hearing, FTC Chairman Pitofsky said the FTC would wait until the end of the year to propose such legislation to give industry one last chance to self regulate. He outlined the framework for such potential legislation at the hearing. Industry representatives defended the pace of their efforts to develop "seals of approval"for Web sites that clearly explain their privacy policies to users and agree to work with organizations overseeing the seals (such as the Better Business Bureau or TRUSTe) to resolve consumer complaints. Representatives of the Center for Democracy and Technology and the Center for Media Education expressed concern that self-regulation was insufficient to protect privacy on the Web. The Direct Marketing Association witness emphasized that many privacy concerns are about "chat rooms" and electronic mail, not Web sites, and each type of Internet usage needs to be treated separately.

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, 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. In a July 31, 1998 statement, he addressed a wide range of privacy issues, reiterating his call for Congress to pass legislation protecting medical records (see CRS Issue Brief 98002), hailing passage of S. 512 (discussed above) as a first step towards dealing with identity theft issues, and asking 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.

Protecting Children from Unsuitable Material and Sexual Predators

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 (see CRS Report 97-841, *Indecency: Restrictions on Broadcast Media, Cable Television, and the Internet)*. In June 1997, the Supreme Court overturned the portions of the CDA dealing with indecency and the Internet. (Existing law still permits criminal prosecutions for transmitting obscenity or child pornography over the Internet.)

Filtering Software. The Clinton Administration, which had sought to uphold the CDA, subsequently proposed an "E-chip" for computers, equivalent in purpose to the V-chip mandated for most television sets in the Telecom Act (see CRS Report 97-43, *V-Chip and TV Ratings: Helping Parents Supervise Their Children's Television Viewing*, for information on the latter). In theory, an "E-chip" would block access by children to Web sites with ratings indicating indecent or otherwise

objectionable material. Unlike the television V-chip, where a single ratings system was developed because of limits on the amount of information that can be transmitted with the broadcast signal, multiple ratings systems could exist for Web sites. Many different organizations could rate a particular Web site, with or without the knowledge and participation of the Web site owner. Parents could set the "E-chip" to screen out Web sites based on the rating system of whatever organization(s) they choose.

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 still uncommon, but may become 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. Three House bills have been introduced to require Internet service providers to offer filtering software to parents: H.R. 774 (Lofgren); H.R. 1180 (McDade); and H.R. 1964 (Markey). The Senate adopted a Dodd amendment to the FY1999 Commerce, State, Judiciary appropriations bill (S. 2260) on July 23 that requires Internet service providers to offer filtering software to customers.

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.

A particular focus of the debate today over filtering systems is schools and libraries. 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.

Senator McCain and Representative Franks introduced bills (S. 1619 and H.R. 3177) to require schools receiving federally-provided "e-rate" subsidies through the

universal service fund to use filtering software to block out Internet sites that might contain material inappropriate for children. (For information on universal service and the e-rate, see CRS Issue Brief 95067, *Telecommunications Regulatory Reform*). Libraries receiving e-rate funds are required to have one or more computers that use filtering software. The determination of what is inappropriate is left to the school, school board, library, or "other authority responsible for making the required certification." Supporters of the requirement for filtering systems argue that children must be protected from inappropriate material, particularly when their parents are not present to supervise them. Opponents argue that it is censorship, that the filtering software also prevents access to appropriate sites, and that such decisions should be left to the local community.

The Senate Commerce Committee reported S. 1619 on June 25 (S. Rept. 105-226). See CRS Report 98-328, *Restrictions on Minor's Access to Material on the Internet*, for a legal analysis of S. 1619 (and S. 1482 as well). The Senate adopted the language of S. 1619 as an amendment to a Coats amendment to the FY1999 Commerce, Justice, State appropriations bill (S. 2260) on July 21. (The Coats amendment concerns commercial distribution via the World Wide Web of material that is harmful to minors, see below). The House Appropriations Committee took a broader approach, adopting an Istook amendment to the FY1999 Labor-HHS appropriations bill (H.R. 4274) that requires schools and libraries to install filtering software if they receive funds under any federal agency program or activity to acquire or operate any computer that is accessible to minors and has access to the Internet.

Prohibiting Material that is "Harmful to Minors". Other legislation has been introduced dealing with indecency or material that is "harmful to minors" on the Internet. S. 1482 (Coats) and H.R. 3783 (Oxley) would prohibit commercial distribution of material that is "harmful material to minors" over the Web. The bills were introduced to replace the provisions of the Communications Decency Act that were overturned by the Supreme Court. By limiting the language to commercial activities, Senator Coats has stated that he hopes to have drafted a bill that will survive court challenges. The Senate Commerce Committee reported the bill on June 25 (S. Rept. 105-225). The language of the bill was adopted as a Coats amendment to the FY1999 Commerce, Justice, State appropriations bill (S. 2260) on July 21. (See CRS Report 98-328, *Restrictions on Minor's Access to Material on the Internet*, for a legal analysis of S. 1482, and S. 1619 as well).

The House adopted a Jackson-Lee amendment to H.R. 3494(McCollum, discussed below) on June 11 that requires the FBI 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.

Sexual Predators on the Internet. There also are legislative efforts to prevent sexual predators from obtaining Internet accounts that could allow them to contact children. 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. One bill in the Senate and one in the House (S. 1356, Faircloth; H.R. 2791, Roukema) would prohibit sexually violent

predators [as defined in section 170101(a)(3) of the Violent Crime Control and Law Enforcement Act of 1994] from obtaining Internet accounts. Another House bill, H.R. 2815 (Weller), would make it a crime to target children for sexually explicit messages or contacts. A Faircloth amendment to the FY1999 Commerce, Justice, State appropriations bill (S. 2260) was adopted on July 22 that gives the FBI administrative subpoena authority in cases involving a federal violation related to sexual exploitation and abuse of children. The provision reportedly is intended to make it easier for the FBI to gain access to Internet service provider records of suspected sexual predators.

H.R. 3494 (McCollum) and S. 1987 (DeWine) would, *inter alia*, prohibit contacting a minor over the Internet for the purposes of engaging in illegal sexual activity, and punish those who knowingly send obscenity to children. Hearings were held by the House Judiciary Committee's Subcommittee on Crime on H.R. 3494, S. 2815, and related legislation on November 7, 1997 and April 30, 1998. H.R. 3494 passed the House on June 11 with a number of amendments added during committee markup on May 6 (H.Rept. 105-557) or on the floor, several of which are discussed elsewhere in this section. In summary, in addition to the language as introduced, H.R. 3494 prohibits individuals from making available by mail or any other means of interstate or foreign commerce personal information about an individual under 18 for facilitating, encouraging, offering, or soliciting sexual activity. It requires electronic communication or remote computing services that have knowledge of violations of child pornography laws to report it to law enforcement officials, prohibits Federal prisoners from having unsupervised access to the Internet, and requires an FBI study of technologies to control the electronic transmission of pornography.

The language of S. 1965 (Moseley-Braun) was adopted as an amendment to the FY1999 Commerce, Justice, State appropriations bill (S. 2260) on July 23. It is similar to language in H. R. 3494 that prohibits individuals from making available personal information about an individual for facilitating, encouraging, offering, or soliciting sexual activity. The Senate language affects individuals under 17, while H.R. 3494 is for individuals under 18.

Other Legislation Related to Protecting Children. As noted, H.R. 3494 contains a number of provisions related to the protection of children. Other House bills also relate to that topic. H.R. 2173 (Franks) would require Internet service providers to report to law enforcement officials instances of suspected child abuse they discover or that are brought to their attention by users. They also would have to turn over any evidence they gathered. The House Judiciary Committee's Subcommittee on Crime held a hearing on H.R. 2173 and related legislation on April 30, 1998. H.R. 2648 (Bachus) would set penalties for possessing more than three items of material containing child pornography that has been transported by various means, including by computer. H.R. 3985 (Lampson) would authorize $2 million per year for FY1999-2002 for the U.S. Customs Service's International Child Pornography Investigation and Coordination Center to deal with the increase in child pornography activities due to the Internet. H.R. 3729 (Pryce) is very similar to language added to H.R. 3494 during markup that prohibits Federal prisoners from having unsupervised access to the Internet.

In the Senate, S. 900 (Feingold) would amend federal sentencing guidelines to enhance a sentence "if the defendant used a computer with the intent to persuade, induce, entice, or coerce a child ... to engage in any prohibited sexual activity." S. 900 was reported from the Senate Judiciary Committee on October 9, 1997 without written report.

Part of the concern about unsuitable material on the Internet involves unsolicited advertising ("junk e-mail") that contains pornography or links to pornographic Web sites (see below).

Industry Response. The Internet community is anxious to avoid legislation. At a "Kids Online Summit" in December 1997, several major players in the Internet industry pledged to do what they could to make the Internet safer for children. America Online (AOL), one of the largest Internet service providers, for example, announced a new policy stating that "when child pornography is appropriately brought to our attention and we have control over it, we will remove it. Subject to constitutional safeguards and statutory privacy safeguards, we will cooperate fully with law enforcement officials investigating child pornography on the Internet." AOL, AT&T, and Microsoft promised to offer filtering software to parents and implement an outreach and educational campaign to increase its use.

Privacy of Personal Information in Government Databases

The growth in the use of the Internet for providing government services raises similar concerns about how to ensure the confidentiality of personal information. Use of computer and telecommunications technologies by government agencies for storing, accessing, and disseminating information offers the advantages of potentially reducing costs, while simultaneously improving customer service. For these reasons, agencies have placed considerable emphasis on developing online access to information and enhancing the ability of citizens to supply information electronically to the government to receive services or comply with rules and regulations. Both the Administration's National Performance Review (NPR) effort and its National Information Infrastructure (NII) initiative emphasized the use of information technology for improving efficiency of government operations, increasing citizen access to government information, and providing better service to individuals.

As these efforts begin to move from the planning to the operational phases, agencies are faced with the need to provide adequate privacy protections for these systems and services. While the Internet offers considerable advantages in terms of the ease with which large numbers of people can interact with agency computer systems, it also lacks security. It is critical for the success of these new "electronic government" initiatives that the public has confidence that personal privacy is not jeopardized. Thus, agencies must develop adequate procedures and apply technological safeguards to ensure that confidentiality of agency records is not compromised.

An example is the development of an online Personal Earnings and Benefit Estimate Statement (PEBES) by the Social Security Administration (SSA). As summarized in its September 1997 report *Social Security: Privacy and Customer Service in the Electronic Age*, the SSA initiated an online PEBES service in March

1997, following earlier pilot testing and after considerable study and developmental work. The system allowed individuals to query the system for their PEBES data and receive instantaneous response over the Internet. People needed to supply five authenticating elements (name, social security number, date of birth, state of birth, and mother's maiden name) to gain access to the data. While these authentication procedures were consistent with what is required using SSA's 800-number and for written requests, there was a strong public response to potential privacy abuses.

The concerns centered on the fact that the authenticating data are readily available from a variety of sources and thus PEBES information could be obtained by those other than the individual whose records would be provided. In response to these concerns, SSA suspended operation of the online PEBES system and held six public forums around the country to solicit comments from experts and interested citizens. Based upon the input received from these forums and other sources, such as congressional hearings, SSA concluded that it would provide a modified version of online PEBES on the Internet with additional security and authentication safeguards early in 1998. Since the law requires SSA to provide, by 1999, PEBES statements each year to all workers 25 and older, SSA considers it a very high priority to establish an online PEBES system that will meet necessary security and privacy standards. It has announced plans to implement additional safeguards using a public key infrastructure in the future.

The SSA example is indicative of a major trend toward greater use of the Internet for these types of government functions. Representative Eshoo has introduced H.R. 2991, the Electronic Commerce Enhancement Act of 1997, to require agencies to create online versions of their forms and make them accessible to the public. This would enable citizens to fill out forms online, return them (along with payments, such as taxes owed), and verify the transactions using digital signature technology (discussed earlier).

Major legislative changes to the welfare, immigration, and health care payments systems also necessitate the creation of large scale databases to monitor the status of applicants for programs. For example, the Personal Responsibility and Work Opportunity Reconciliation Act, P.L. 104-193 (welfare reform), establishes new federal databases for all new hires nationwide, quarterly wage reports of all working persons, unemployment insurance data, and lists of people who owe or are owed child support. The first component of this system, the National Directory of New Hires, recently went into operation and requires every state to send data on new hires daily to the Department of Health and Human Services (HHS). The goal of this system is to track parents who are overdue on their child support payments, but some privacy advocates are concerned that it might be used for purposes beyond those identified in the statute, such as other government agencies using it to verify eligibility for benefits programs.

The Illegal Immigration Reform and Immigrant Responsibility Act (P.L. 104-208) required enhancements to the systems used to monitor immigration into the United States in an effort to thwart illegal immigration. As required by the law, the Immigration and Naturalization Service (INS) has begun implementing new digital "green cards", which store digitized fingerprints, a digital photo, and a digital signature. The Health Insurance Portability and Accountability Act (P.L. 104-191)

established requirements for the use of standard electronic transactions for activities such as the submissions of health insurance financial claims and transmission of payment and remittance advice. (See CRS Issue Brief 98002, *Medical Records Confidentiality*, for a discussion of those issues and related legislation: H.R. 52, H.R. 1815, H.R. 3900, S. 1368, and S. 1921). These developments, combined with efforts to move towards more electronic benefits delivery systems, reinforce the need for effective mechanisms to protect confidentiality and ensure system security in government computer operations.

In a broad speech on Internet privacy issues on May 14, Vice President Gore announced the release of a memorandum for heads of executive department and agencies outlining steps agencies must take to ensure that the expanded use of information technologies does not erode privacy protections already provided in statute.

Intellectual Property

The era of global Internet connectivity presents significant challenges to effectively protecting the rights of copyright holders. Computers can make exact duplicates of originals and networks can provide access to literally millions of individuals. Some observers maintain that the growth of international computer networks will depend, in part, upon the willingness of individuals and businesses to make information available electronically. Absent adequate intellectual property protection, authors and publishers often are reluctant to provide Internet access to material of value. Some experts contend that technological solutions, such as encryption, digital signatures, digital watermarks, and other verification software, will address these concerns. Others suggest that the existing legal regime for intellectual property rights is inadequate for addressing the electronic distribution of material and must be replaced with different approaches to fostering creativity in the digital environment. Many maintain that existing legal authorities can and should be modified to account for the changing technological scene and recommend expanding the current legal framework to encompass the transmission of digital information.

Legislation is moving through Congress that addresses three aspects of intellectual property rights in the digital era: implementation of two World Intellectual Property Organization (WIPO) treaties; copyright infringement liability protection for Online Service Providers (OSPs); and copyright protection of collections of information (databases). As the debate has evolved during the 105th Congress, various bills have merged with or been replaced by others. Currently, all three issues are combined in H.R. 2281, which passed the House on August 4. In the Senate, WIPO implementation and OSP liability are in S. 2037, which passed the Senate on May 14, while database protection issues are in S. 2291 on which hearings have not yet been held.

WIPO Implementation

The House and Senate have each passed legislation (H.R. 2281 and S. 2037) to implement two new World Intellectual Property Organization (WIPO) treaties adopted in Geneva in December 1996 — the WIPO Performances and Phonograms

Treaty and the WIPO Copyright Treaty. The bills amend the Copyright Act to prohibit the circumvention of anti-copying technology and assure the integrity of copyright management information systems. Alternative House (H.R. 3048, Boucher) and Senate (S. 1146, Ashcroft) bills to implement the WIPO treaties were introduced that have somewhat different language concerning circumvention of anti-copying technologies and copyright management information systems, and including provisions related to use of copyrighted digital material by teachers and librarians. (See CRS Report 97-444, *World Intellectual Property Organization Copyright Treaty: An Overview*.) Librarians were particularly concerned that the circumvention language would mean that users had to pay each time they copied a small portion of a work on the Internet. As passed, H.R. 2281 delays implementation of that provision for two years, during which time the Secretary of Commerce is to study its impact on fair use. The Secretary could waive the ban where fair use would be harmed. In the Senate, the Judiciary Committee considered S. 1121 and S. 1146 on April 30 and ordered reported a new bill, S. 2037, incorporating provisions from both. That bill passed the Senate on May 14.

Online Service Provider Liability Protection

S. 2037 and H.R. 2281 also cover copyright infringement liability of online service providers (OSPs)[1]. That debate focuses on the legal liability of the OSPs in situations where they act strictly as conduits for material that infringes on copyright. While copyright holders generally assert that existing copyright law is adequate to deal with the issue of OSP liability, others in the telecommunications industry and the academic and library communities advocate new legislation to specify the OSP exemption from liability. (See CRS Report 97-950, *Online Service Provider Copyright Liability: Analysis and Discussion of H.R. 2180 and S. 1146*.) Both the Senate and House bills as passed exempt OSPs from liability if they act only as conduits of information.

Database Protection

Legislation covering the issue of database protection is also being considered. The Collections of Information Antipiracy Act (H.R. 2652, Coble), passed the House on May 19 and than was also attached to H.R. 2281 when it passed the House August 4. A Senate bill, S. 2291 (Grams), was introduced July 10, 1998. The House bill was the subject of hearings by the Subcommittee on Courts and Intellectual Property of House Judiciary on October 23, 1997 and February 12, 1998. The decision to attach the database protection bill (H.R. 2652) to the WIPO implementation/OSP liability protection bill (H.R. 2281) in the House is controversial. Critics who have concerns about the database provisions, including major scientific and library associations and the Clinton Administration, argue that the issue may prevent the rest of the bill from being enacted. The Clinton Administration has raised constitutional questions about Congress' authority to enact such legislation.

---

[1] The OSP provisions of H.R. 2281 originated in H.R. 2180, that itself was superseded by H.R. 3209. They were merged into H.R. 2281 during markup by the House Judiciary Committee on April 1, 1998.

The issue is very controversial. Scientific groups and the library community have cautioned against establishing new protections for databases that might compromise fair use and access to data for scientific research. Among the issues they have raised are whether a need for a new intellectual property right has been adequately demonstrated, the definition of key term such as "database" that might encompass a broader array of information than what would be necessary to protect competition in the information industry, and the importance of ensuring that information produced by government employees remains publicly available, free from copyright restrictions.

Database producers argue that the compilation of factual databases requires some form of protection beyond current law if companies could be expected to make substantial investments in creating them. The ability to download and retransmit data over the Internet facilitates copying of information, making producers of factual, noncopyrightable, databases more vulnerable. They argue that the absence of some form of database-specific property rights has a chilling effect on the database industry that would result in fewer factual databases being compiled and thus could potentially reduce the availability of information to the public.

Unsolicited Commercial Electronic Mail ("Junk E-Mail" or "Spamming")

Another 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 "spamming," "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 June 17, 1998 hearing on spamming before the Senate Commerce Committee, America Online (AOL) stated that junk e-mail represents 5-30% of the 15 million Internet e-mail messages it handles each day.

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."

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.

The Senate adopted a Murkowski-Torricelli amendment to S. 1618, the Anti-slamming Amendments Act, that follows the "opt-out" philosophy and reflects provisions in S. 771 (Murkowski) and S. 875 (Torricelli). Senders of commercial e-mail would have to clearly identify in the subject line of the message that it is an advertisement, require Internet service providers to make software available to their subscribers to block such e-mail, and prohibit sending e-mail to anyone who has asked not to receive such mail. Similar language was included in the House version of the Anti-slamming bill, H.R. 3888, which was marked up by the House Commerce Telecommunications Subcommittee on August 6. Concerns were raised by several subcommittee members that the language might infringe on First Amendment rights, however, and commented that they wanted more information before proceeding with the bill because of that and other issues. Four other House bills also address the issue. H.R. 1748 (Smith) would amend the 1991 Telephone Consumer Protection Act to treat junk e-mail the same as junk fax. H.R. 2368 (Tauzin) would encourage industry to establish voluntary guidelines for transmission of junk e-mail. H.R. 4124 (Cook) and H.R. 4176 (Markey) reflect the opt-out approach.

As noted earlier, some unsolicited e-mail either contains indecent material or provides links to other sites where indecent material is available. Thus, controls over junk e-mail have also arisen in the context of protecting children from unsuitable material. In October 1997, AOL filed suit to prevent a company that sends unsolicited e-mails offering "cyberstrippers" from sending e-mail to AOL subscribers. The company, Over the Air Equipment, agreed on December 18, 1997 to drop its challenge to a preliminary injunction barring it from sending such advertisements to AOL subscribers (Reuters, Dec. 18, 1997, 11:57 AET).

Internet Domain Names

Another Internet issue before the 105th Congress is Internet domain names. 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 controversial. The House Science Committee held hearings on Internet domain name

issues on September 25 and 30, 1997, and March 31, 1998. Among the issues are governance of the domain name system, how to foster competition in domain name registration services, and approaches to resolving trademark disputes that arise in designating domain names. The latter topic was the subject of hearings before the House Judiciary Committee's Subcommittee on Courts and Intellectual Property on November 5, 1997 and February 12, 1998. A bill was introduced on March 6 (S.1727) by Senator Leahy to authorize a comprehensive independent study of the effects on trademark and intellectual property rights holders of adding new generic top-level domains and related dispute resolution procedures.

The domain name issue is discussed in more detail in CRS Report 97-868, *Internet Domain Names: Background and Policy Issues*. Briefly, in 1993, the National Science Foundation (NSF) entered into a 5-year cooperative agreement with Network Solutions, Inc (NSI) to operate Internet domain name registration services. In 1995, the agreement was modified to allow NSI to charge registrants a $50 fee per year for the first two years, of which 70% goes to NSI to cover its costs and 30% is deposited in the "Intellectual Infrastructure Fund" to be reinvested in the Internet.

The cooperative agreement between NSF and NSI expired on March 31, 1998, but was automatically extended for six months while decisions are made on how to handle domain name registration in the future. There has been criticism of NSI's exclusive control over registration of domain names and an increase in trademark disputes over name registrations in the ".com" domain that identifies businesses.

On January 30, 1998, the Department of Commerce released a "discussion draft" entitled *Proposal to Improve Technical Management of Internet Names and Addresses* (called the "green paper") setting forth the Administration's proposal to privatize administration of the domain name system (DNS). A new private, not-for-profit corporation would be created to which the U.S. government would transition authority for domain name registration, with operational responsibility transferred by September 1998. The new corporation would serve a policy-setting role and administer certain technical aspects of Internet operation (direct allocation of Internet Protocol number blocks, and oversight of the Internet root server system, for example). The U.S. government would participate in policy oversight of the new corporation during a transition period ending no later than September 2000. Also, five new "generic top level domains" (such as .com) would be created and five registries to oversee them (one for each). Thus there would be six domain name registries: NSI and the five new entities. There would be no limit on the number of "registrars" who would act as the interface between an Internet user and the registries.

Several parts of the Administration plan were opposed by many parties during the public comment period. Many expressed concern that under the new policy, the U.S. government would have a greater degree of control than foreign governments over DNS management. At a House Science Committee hearing on March 31, 1998, strong opposition to the green paper was voiced by the Internet Council of Registrars (CORE). An association of 87 companies, CORE was established in 1996 to manage the master database of domain names and the main computer servers that route address information around the world. CORE has proposed a 10-point plan that would, among other things, create seven new categories of generic top level

domains, instead of five as recommended in the green paper. A single non-profit registry would control all the generic top level domains instead of the six registries proposed in the green paper. Other witnesses also expressed reservations about the Department's proposal.

On June 5, the Administration released a "white paper" policy statement called the *Management of Internet Names and Addresses*, which affirms many of the proposals in the green paper. On June 10, the House Subcommittee on Telecommunications, Trade and Consumer Protection held a hearing to review private sector concerns over the policy. Most witnesses stated that the policies outlined in the white paper are less complex than in the green paper, and leave many of the DNS management decisions to the private sector rather than government.

NSF's authority to require the collection of monies that have been set aside in the Intellectual Infrastructure Fund and the disposition of that money are also controversial. As of March 31, 1998, $56 million had been collected. In the FY1998 appropriation bill that includes NSF (P.L.105-65), Congress allocated $23 million of the monies in the fund to NSF's Research and Related Activities account to support development of the Next Generation Internet. However, the legality of NSF's creation of the infrastructure fund is being debated in the U.S. District Court for the District of Columbia. A preliminary injunction prevents NSF from spending the money. The suit claims that NSF lacks the authority to authorize NSI to collect fees for domain name registration services and the money should be refunded to users.

On April 6, 1998, U.S. District Judge Thomas Hogan dismissed the charge that NSF lacked authority to permit NSI to collect fees, but let stand another charge challenging the portion of the fee collected for the infrastructure fund. Meanwhile, NSF and NSI have discontinued collecting fees for the infrastructure fund in accordance with the January 30 green paper's recommendation that allocating part of the registration fee to the infrastructure fund end on April 1, 1998.

105th Congress Legislation

(*NOTE*: MANY BILLS WOULD FIT UNDER SEVERAL DIFFERENT CATEGORIES. THEY ARE CATEGORIZED HERE BASED ON EACH BILL'S MAJOR THRUST IN THE CONTEXT OF THE TOPICS DISCUSSED IN THIS REPORT. COMMITTEES TO WHICH THE BILLS HAVE BEEN REFERRED ARE NOTED IN PARENTHESES.)

Encryption and Digital Signatures

H.R. 695, Goodlatte, Safety and Freedom Through Encryption (JUDICIARY, INTERNATIONAL RELATIONS, NATIONAL SECURITY, INTELLIGENCE, COMMERCE)
H.R. 2937, Baker, Electronic Financial Services Efficiency Act (COMMERCE, GOVERNMENT REFORM AND OVERSIGHT, JUDICIARY, SCIENCE, BANKING AND FINANCIAL SERVICES)
H.R. 2991, Eshoo, Electronic Commerce Enhancement Act (GOVERNMENT REFORM AND OVERSIGHT, COMMERCE)

S. 376, Leahy, Encrypted Communications Privacy Act (JUDICIARY)
S. 377, Burns, Promotion of Commerce On-Line in the Digital Era (COMMERCE, SCIENCE, AND TRANSPORTATION)
S. 909, McCain, Secure Public Networks Act (COMMERCE, SCIENCE, AND TRANSPORTATION)
S. 1594, Bennett, Digital Signature and Electronic Authentication Law (BANKING)
S. 2067, Ashcroft, Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace (JUDICIARY)
S. 2107, Abraham, Electronic Commerce Enhancement Act (COMMERCE)

Computer Security (General)

H.R. 1903, Sensenbrenner, Computer Security Enhancement Act (SCIENCE)

S. 2303, Leahy, International Crime Control Act (JUDICIARY)

Computer Privacy (General)

H.R. 98, Vento, Consumer Internet Privacy Protection (COMMERCE)
H.R. 1287, Bob Franks, Social Security On-line Privacy Protection (COMMERCE)
H.R. 1330, Kanjorski, American Family Privacy (GOVERNMENT REFORM AND OVERSIGHT)
H.R. 1331, Kennelly, Social Security Information Safeguards (WAYS AND MEANS)
H.R. 1367, Barrett, Federal Internet Privacy Protection (GOVERNMENT REFORM AND OVERSIGHT)
H.R. 1813, Kleczka, Personal Information Privacy (WAYS AND MEANS, BANKING AND FINANCIAL SERVICES, JUDICIARY)
H.R. 1964, Markey, Communications Privacy and Consumer Empowerment (COMMERCE)
H.R. 1972, Bob Franks, Children's Privacy Protection and Parental Empowerment (JUDICIARY)

H.R. 2368, Tauzin, Data Privacy Act (COMMERCE)
H.R. 3551, DeLauro, Identity Piracy Act (JUDICIARY, TRANSPORTATION AND INFRASTRUCTURE)
H.R. 3601, Shadegg, Identity Theft and Assumption Deterrence Act (JUDICIARY, TRANSPORTATION AND INFRASTRUCTURE)
H.R. 4151, Shadegg, Identity Theft and Assumption Deterrence Act (JUDICIARY)

S. 504, Feinstein, Children's Privacy Protection and Parental Empowerment (JUDICIARY)
S. 512, Kyl, Identify Theft and Assumption Deterrence Act (JUDICIARY)
S. 600, Feinstein, Personal Information Privacy (FINANCE)
S. 2326, Bryan, Children's Online Privacy Protection Act (COMMERCE)

Computer Privacy (Protecting Children from Pornography, Predators)

Filtering

HR 774, Lofgren, Internet Freedom and Child Protection (COMMERCE)
HR 1180, McDade, Family-Friendly Internet Access (COMMERCE)
H.R. 3177, Franks, Safe Schools Internet Act (COMMERCE)
H.R. 4274, Porter, FY1999 Labor-HHS Appropriations Act (APPROPRIATIONS) *[amendment re filtering added during committee markup]*

S. 1619, McCain, Internet School Filtering Act (COMMERCE) *[Incorporated into S. 2260, Commerce, Justice, State appropriations, during floor debate]*
S. 2260, Gregg, FY1999 Commerce, Justice, State Appropriations Act (APPROPRIATIONS) *[As passed, incorporates S. 1619 plus separate Dodd amendment re filtering]*

Other

H.R. 2173, Franks, Child Abuse Notification Act (JUDICIARY)
H.R. 2648, Bachus, Abolishing Child Pornography Act (JUDICIARY)
H.R. 2791, Roukema, Prohibition on Provision of Internet Service Accounts to Sexually Violent Predators (COMMERCE)
H.R. 2815, Weller, Protecting Children from Internet Predators (JUDICIARY)
H.R. 3494, McCollum, Child Protection and Sexual Predator Punishment Act (JUDICIARY)
H.R. 3729, Pryce, Stop Trafficking of Pornography in Prisons (JUDICIARY) *[Virtually identical language adopted as Chabot amendment to H.R. 3494 during Judiciary committee markup of that bill.*]
H.R. 3783, Oxley, Child Online Protection Act (COMMERCE)
H.R. 3985, Lampson, Authorize Appropriations for International Child Pornography Investigation and Coordination Center of the Customs Service (WAYS AND MEANS)

S. 900, Feingold, Child Exploitation Sentencing Enhancement Act (JUDICIARY)
S. 1356, Faircloth, Prohibition on Provision of Internet Service Accounts to Sexually Violent Predators (COMMERCE, SCIENCE AND TRANSPORTATION)
S. 1482, Coats, Prohibition of Commercial Distribution on the World Wide Web of Material That is Harmful to Minors (COMMERCE) *[Incorporated into S. 2260, Commerce, Justice, State Appropriations Act]*
S. 1965, Moseley-Braun, Internet Predator Prevention Act (JUDICIARY) *[Incorporated into S. 2260, Commerce, Justice, State Appropriations Act]*
S. 1987, DeWine, Child Protection and Sexual Predator Punishment Act (JUDICIARY)

Computer Privacy (Medical Records Confidentiality)

H.R. 52, Condit, Fair Health Information Practices Act (COMMERCE, GOVERNMENT REFORM AND OVERSIGHT, JUDICIARY)
H.R. 1815, McDermott, Medical Privacy in the Age of Technologies Act (COMMERCE, GOVERNMENT REFORM AND OVERSIGHT)
H.R. 3900, Shays, Consumer Health and Research Technology Protection Act (COMMERCE, WAYS AND MEANS, GOVERNMENT REFORM AND OVERSIGHT)

S. 1368, Leahy, Medical Information Privacy and Security Act (LABOR AND HUMAN RESOURCES)
S. 1921, Jeffords, Health Care Personal Information Nondisclosure Act (LABOR AND HUMAN RESOURCES)

Intellectual Property

*H.R. 2180, Coble, On-Line Copyright Liability Limitation Act (JUDICIARY)
*H.R. 2281, Coble, WIPO Copyright Treaties Implementation Act (JUDICIARY)
H.R. 2652, Coble, Collections of Information Antipiracy Act (JUDICIARY)
H.R. 3048, Boucher, Digital Era Copyright Enhancement Act (JUDICIARY)
*H.R. 3209, Coble, On-Line Copyright Infringement Liability Limitation Act (JUDICIARY)
[H.R. 2180 and H.R. 3209 were merged into H.R. 2281 during markup.]*

*S. 1121, Hatch, WIPO Copyright and Performances and Phonograms Treaty Implementation Act of 1997 (JUDICIARY)
*S. 1146, Ashcroft, Digital Copyright Clarification and Technology Education Act of 1997 (JUDICIARY)
*S. 2037, Hatch, Digital Millenium Copyright Act (JUDICIARY)
[**S. 2037 replaces S. 1121 and S. 1146.]*
S. 2291, Grams, Collections of Information Antipiracy Act (JUDICIARY)

Unsolicited E-mail

H.R. 1748, Christopher Smith, Netizens Protection Act (COMMERCE)
H.R. 3888, Tauzin, Anti-Slamming Amendments (COMMERCE)
H.R. 4124, Cook, E-Mail User Protection Act (COMMERCE)
H.R. 4176, Markey, Digital Jamming Act, (COMMERCE)

*S. 771, Murkowski, Unsolicited Commercial Electronic Mail Choice Act (COMMERCE, SCIENCE, AND TRANSPORTATION)
*S. 875, Torricelli, Electronic Mailbox Protection Act (COMMERCE, SCIENCE, AND TRANSPORTATION)
*S. 1618, McCain, Anti-Slamming Amendments (COMMERCE, SCIENCE, AND TRANSPORTATION)
* *[S. 771 and S. 875 were incorporated into S. 1618 during floor debate]*

Internet Domain Names

S. 1727, Leahy, to authorize the comprehensive independent study of the effects of trademark and intellectual property rights holders of adding new generic top-level domains and related dispute resolution procedures (JUDICIARY)

Related CRS Reports

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.

"Digital Era Copyright Enhancement Act": Analysis of H.R. 3048, by Dorothy Schrader. CRS Report 98-520 A. 8 p. May 18, 1998.

Encryption and Banking, by M. Maureen Murphy. 12 p. CRS Report 97-835 A. September 15, 1997.

Encryption Export Controls, by Jeanne J. Grimmett. 6 p. CRS Report 97-837 A. September 12, 1997.

Encryption, Key Recovery & Law Enforcement: Selected Legal Issues and Legislative Proposals, by Charles Doyle. 41 p. CRS Report 97-845 A. September 12, 1997.

Encryption Technology and U.S. National Security, by Michael Vaden and Edward Bruner. 9 p. CRS Report 96-670 F. August 8, 1996.

Encryption Technology: Congressional Issues, by Richard Nunno. CRS Issue Brief 96039. 15 p. (Updated Regularly)

Indecency: Restrictions on Broadcast Media, Cable Television, and the Internet, by Henry Cohen. CRS Report 97-841 A. 14 p. September 12, 1997.

Information Privacy, by Gina Marie Stevens. CRS Report 97-833 A. 13 p. September 15, 1997.

Internet Domain Names: Background and Policy Issues, by Jane Bortnick Griffith. CRS Report 97-868 SPR. 6 p. March 30, 1998.

Internet Technology, by Ivan Kaminow and Jane Bortnick Griffith. CRS Report 97-392 SPR. 6 p. December 24, 1997.

Medical Records Confidentiality, coordinated by Irene Stith-Coleman. CRS Issue Brief 98002. 15 p. (Updated Regularly)

Next Generation Internet, by Glenn J. McLoughlin. CRS Report 97-521 STM. 6 p. June 8, 1998.

Online Service Provider Copyright Liability: Analysis and Discussion of H.R. 2180 and S. 1146, by Dorothy Schrader. CRS Report 97-950 A. 15 p. April 14, 1998.

Protecting Privacy on the Internet: A Summary of Legislative Proposals, by Angela Choy, Marcia Smith, and Jane Bortnick Griffith. CRS Report 97-1061 STM. 6 p. December 19, 1997.

Restrictions on Minor's Access to Material on the Internet, by Henry Cohen. CRS Report 98-328 A. 6 p. July 16, 1998.

Telecommunications Regulatory Reform, by Angele Gilroy. CRS Issue Brief 95067. 19 p. (Updated Regularly).

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

Welcome to Cyberia: An Internet Overview, by Rita Tehan. CRS Report 97-544 C. 18 p. May 12, 1997.

World Intellectual Property Organization Copyright Treaty: An Overview, by Dorothy Schrader. CRS Report 97-444 A. 24 p. April 14, 1998.

WIPO Copyright Treaty Implementation Legislation: Recent Developments, by Dorothy Schrader. CRS Report 98-463. 7 p. May 14, 1998.

World Intellectual Property Organization Performance and Phonograms Treaty: An Overview, by Dorothy Schrader. CRS Report 97-523. 32 p. April 14, 1998.