

**Calendar No. 551**

107TH CONGRESS }  
2d Session }

SENATE

{ REPORT  
107-240

**ONLINE PERSONAL PRIVACY ACT**

---

R E P O R T

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND  
TRANSPORTATION

ON

S. 2201

TOGETHER WITH

MINORITY VIEWS



AUGUST 1, 2002.—Ordered to be printed

---

U.S. GOVERNMENT PRINTING OFFICE

99-010

WASHINGTON : 2002

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

ERNEST F. HOLLINGS, South Carolina, *Chairman*

DANIEL K. INOUE, Hawaii	JOHN McCAIN, Arizona
JOHN D. ROCKEFELLER IV, West Virginia	TED STEVENS, Alaska
JOHN F. KERRY, Massachusetts	CONRAD BURNS, Montana
JOHN B. BREAUX, Louisiana	TRENT LOTT, Mississippi
BYRON L. DORGAN, North Dakota	KAY BAILEY HUTCHISON, Texas
RON WYDEN, Oregon	OLYMPIA J. SNOWE, Maine
MAX CLELAND, Georgia	SAM BROWNBACK, Kansas
BARBARA BOXER, California	GORDON SMITH, Oregon
JOHN EDWARDS, North Carolina	PETER G. FITZGERALD, Illinois
JEAN CARNAHAN, Missouri	JOHN ENSIGN, Nevada
BILL NELSON, Florida	GEORGE ALLEN, Virginia

KEVIN D. KAYES, *Staff Director*

MOSES BOYD, *Chief Counsel*

GREGG ELIAS, *General Counsel*

JEANNE BUMPUS, *Republican Staff Director and General Counsel*

ANN BEGEMAN, *Republican Deputy Staff Director*

## Calendar No. 551

107TH CONGRESS }  
2d Session }

SENATE

{ REPORT  
{ 107-240

---

---

### ONLINE PERSONAL PRIVACY ACT

---

AUGUST 1, 2002.—Ordered to be printed

---

Mr. HOLLINGS, from the Committee on Commerce, Science, and  
Transportation, submitted the following

### REPORT

together with

### MINORITY VIEWS

[To accompany S. 2201]

The Committee on Commerce, Science, and Transportation, to which was referred the bill (S. 2201) to protect the online privacy of individuals who use the Internet, having considered the same, reports favorably thereon with an amendment in the nature of a substitute, and recommends that the bill as amended do pass.

#### PURPOSE OF THE BILL

The purposes of this legislation, as reported, are to create baseline privacy protections for individuals using the Internet that promote privacy, boost consumer confidence, and in turn promote e-commerce as more and more business is conducted online. The privacy protections required in the bill are designed to give individuals: notice of online entities' privacy policies; chances to opt out or opt in to the information practices described in those policies (depending on the sensitivity of the personal information sought by the online entities); reasonable access to personal information collected by online entities; reasonable security for personal information once collected; and a set of enforcement tools to ensure compliance with this framework.

#### BACKGROUND AND NEEDS

##### CONSTITUTIONAL AND LEGAL PROTECTIONS OF PRIVACY

Government sanctioned protection of privacy has a long and documented history in American legal and statutory jurisprudence. In-

deed, concerns about privacy protection date back to the founding fathers, who evidenced their desire to protect privacy in the Bill of Rights. The most notable example in the U.S. Constitution resides in the Fourth Amendment's prohibition of arbitrary searches and seizures of persons and their property.

Recently, this doctrine was determined by the Supreme Court to apply in a case where advanced technology enabled the police to invade the privacy of an individual's home and conduct a search without actually entering the premises. Specifically, this matter was addressed in *Kyllo v. United States*, 533 U.S. 27, (2001), where the Supreme Court invalidated a search of a suspect's home where the police used a thermal-imaging device to search a suspect's residence for evidence that he was growing marijuana.

In its 5-4 ruling, the Court declared that notions of privacy must adapt as technology evolves noting that: "It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology. \* \* \* The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy." 533 U.S. at 33-34.

Notably, the Court concluded that limits must exist on the ability of technology to infringe upon citizens' privacy. Although the decision related to government action, it nevertheless was the first decision to lay down a broad principle as it concerns the relationship of privacy with modern technology. The court stated: "[T]here is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that exists, and that is acknowledged to be reasonable. \* \* \* We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without 'physical intrusion into a constitutionally protected area' \* \* \* constitutes a search \* \* \*. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Id.* at 34 (quoting *Silverman v. United States*, 365 U.S. 505, 512 (1961)).

Aside from the Fourth Amendment and the Bill of Rights, the notion of a distinct legal right to privacy arose at the conclusion of the 19th Century, as journalism and photography combined to generate a desire for common law privacy rights. Prominent 19th Century judges and lawyers popularized one familiar definition of the right to privacy: "the right to be let alone," a phrase made famous by Justice Brandeis in *Olmstead v. United States*, 277 U.S. 438, 478, (1928).

#### U.S. STATUTORY PROTECTIONS OF PRIVACY

Toward the close of the 20th Century, as people's personal information was increasingly collected, profiled, and shared for commercial purposes, and as technology advanced to facilitate these practices, Congress passed numerous statutes designed to protect privacy. Taken as a group, existing privacy laws demonstrate that Congress typically requires privacy protections when new technologies or industries begin to threaten privacy. These laws apply to the government, telephones, cable television, e-mail, video tape rentals, and the Internet (with respect to children). Taken together, these laws appear designed not to limit technology or stifle a new

business, but rather to ensure that certain types of information collection are fair, transparent, and subject to law. Brief summaries of many of these statutes are set forth below (if noted, the statute provides for a private right of action):

The Federal Wiretap Act of 1968, 18 U.S.C. 2510 et. seq., limits the monitoring of private communications.

The Fair Credit Reporting Act of 1970, 15 U.S.C. 1681 et seq., limits the disclosure of information contained in credit reports, requires the credit reporting agency to ensure the information is correct and timely, and affords individuals the right to inspect and correct their credit report.

The Privacy Act of 1974, 5 U.S.C. 552 et. seq., established a legal framework for records collected by the Federal government and responded to the concern raised by monitoring and government use of automated databases.

The Cable Act of 1984, 47 U.S.C. 551 et seq., is the most comprehensive law protecting privacy across a technological medium. Specifically, it allows cable companies to disclose names and subscriber lists only after affording users notice on an annual basis and an opportunity to opt out of such disclosure. Moreover, it prohibits the sharing of viewers' viewing habits unless they provide notice on an annual basis and obtain prior written or electronic consent (i.e. an opt-in). The Act also grants reasonable access to personal information collected and a reasonable opportunity to correct that information. In addition, the statute requires cable operators to destroy personal information if it is no longer necessary for the purpose for which it was collected. Finally, it provides for a private right of action to recover statutory damages in the event of a violation.

The Video Privacy Protection Act of 1988, 18 U.S.C. 2701 et. seq., prohibits sharing or sale of customer lists, unless notice and an opportunity to opt out has been granted, and prohibits sharing or sale of specific video viewing habits without notice and prior consent (i.e. an opt-in). Although the Act does not afford a right of access to information collected about consumers, it does create a private right of action to recover statutory damages in the event of a violation.

The Telephone Consumer Protection Act of 1991, 47 U.S.C. 152 et. seq., which prohibits telemarketers from contacting individuals once they have asked not to be contacted, and entirely prohibits companies from faxing commercial solicitations to individuals with whom they have no prior relationship. This law also provides for a private right of action in the event of a violation.

The Telecommunications Act of 1996's Customer Proprietary Network Information (CPNI) rules, 15 U.S.C. 79 et. seq., which prohibits telephone companies from sharing information about their customers' telephone usage without their approval.

The Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. 6501 et. seq., which prohibits companies on the Internet from collecting and using personal information about children under 13 years of age without notice, and obtaining prior consent (opt in) from parents. Parents can access information collected about their children, and enforcement is conducted by the Federal Trade Commission (FTC) and the Attorneys General.

The Financial Services Modernization Act of 1999 (commonly referred to as Gramm-Leach-Bliley), 12 U.S.C. 24a et. seq., which requires financial institutions to provide customers notice and the opportunity to opt out of industry practices of sharing their financial information with third parties.

The Health Insurance Portability and Accountability Act (HIPAA), 42 U.S.C. 1320d et seq., requires health care providers who transmit health information in electronic transactions, health plans and health care clearinghouses to (i) provide notice of all uses and disclosures of individually identifiable health information transmitted in any form or medium, whether oral, written, or electronic; (ii) obtain prior, written consent (i.e. an opt-in) before using or disclosing protected health information, except in certain circumstances; (iii) provide access to individuals to review data, request corrections and get accounting of all uses and disclosures; and (iv) limit most disclosures, other than for treatment, to only the “minimum necessary” for information. HIPAA also sets forth rules for business associates of any covered entity hired for collection or processing of protected health information. Covered entities may use or disclose protected health information without a consent or authorization only if the use or disclosure comes within one of the listed exceptions, such as for public health reasons, law enforcement, research or to facilitate organ transplants. Exceptions are also made for certain marketing purposes, but individuals must be given notice and an opportunity to opt out.

S. 2201 overlaps with these existing statutes to varying degrees since they all, with the exception of COPPA, apply to information collected both online or offline. For example, a cable company providing Internet access service or a financial institution with a commercial website—while covered by this legislation—also fall under the Cable Act of 1984, and the Gramm-Leach-Bliley Act, respectively. This legislation addresses these overlapping statutory regimes differently, depending on the level of privacy protection in the prior existing statute. Therefore, this legislation either preserves or is reconciled with the pro-privacy provisions in the Cable Act, the Telecommunications Act’s CPNI rules, the Fair Credit Reporting Act, and the Children’s Online Privacy Protection Act. On the other hand, this legislation largely supersedes, with some exceptions, the privacy rules in Gramm-Leach-Bliley and HIPAA, as discussed below, as they apply to the Internet. Testimony before the Committee by consumer organizations has demonstrated that the opt-out notices distributed pursuant to Gramm-Leach-Bliley have failed to help consumers make an informed choice in protecting their sensitive personally identifiable information. Specifically, that testimony stated that in many instances financial institutions have sent cover letters professing their commitment to protect privacy, while simultaneously attaching confusing notices explaining their intent to share people’s personal financial information with numerous third parties. In many of these notices, it is also difficult to determine how to opt out. Evidence of this lack of protection warrants corrective measures to at least ensure adequate privacy for sensitive personal financial information on the Internet. The legislation reported by this Committee would provide such protection.

With respect to sensitive personally identifiable health and medical information, the final HIPAA rules were published on December 28, 2000, and first went into effect on April 14, 2001. All covered entities (except small health plans that have until 2004 to comply) must be in full compliance with the HIPAA rules by April 14, 2003. HIPAA expressly permits the U.S. Department of Health and Human Services (HHS) to review and propose modifications to the rules annually. On March 27, 2002, HHS published proposed rule modifications, many of which were identified by HHS in its guidance on the privacy rules issued in July 2001 as a result of five years of deliberation with interested parties, including industry representatives, academics and consumer advocates. Some consumer privacy advocates have expressed concern over the impact of the proposed revisions on the privacy afforded individuals' sensitive health or medical information. Although these proposed changes have not yet been adopted, the HIPAA rules published in 2000 are still in effect and the compliance deadline is unchanged. It is the opinion of a minority of the Committee members that many of the provisions of S. 2201, if enacted into law, would be in direct conflict with the HIPAA rules, and a covered entity would be unable to comply with both laws.

Because the health privacy rules that derived from HIPAA are currently under review and subject to revision, the majority of the Committee cannot conclusively determine at this time the extent to which to preserve or reconcile those rules in this legislation. It is the Committee's intent in all instances, however, to permit legitimate business activity that necessarily involves sharing of personally identifiable information so long as such sharing is tied—even indirectly—to the purpose for which the information was initially proffered by the individual.

With respect to those industries that criticize this legislation because it imposes overlapping, or distinct privacy regimes, the Committee notes that compliance with this legislation as to specific activities involving the collection of personally identifiable information, in most instances, will also result in compliance with most existing privacy laws in place today.

#### THE EUROPEAN UNION PRIVACY DIRECTIVE AND THE EUROPEAN UNION SAFE HARBOR

In contrast to America's sectoral approach to protecting privacy, Europe recently adopted a comprehensive and overarching privacy protection regime that governs the entire marketplace regardless of whether collection, use or disclosure is online or offline. In 1995, the European Union authored a directive requiring its individual member states to adopt laws reflecting the Directive's privacy protections. The Directive became effective on October 24, 1998. A substantial majority of the 15 member states have adopted laws at least as strong as the Directive, although Sweden, Germany, and Great Britain have each called for simpler, more flexible, and less prescriptive rules than the present Directive. At a minimum, those laws in compliance with the Directive obligate companies, in both their online and offline practices, to provide: (1) notice; (2) an opt-out with respect to non-sensitive commercial marketing of personal information; (3) an opt-in with respect to sensitive personal infor-

mation; (4) a right of access to personal information collected; and (5) reasonable security protections for that information.

To address U.S. industries' concerns about the application of the Directive to American companies—and in particular their fear that they might have to comply with 15 different member state interpretations of the Directive—the Department of Commerce developed a “safe harbor” set of requirements which U.S. companies can meet to comply functionally with the Directive in the member states. The Safe Harbor was approved by the European Union in July 2000. So far, over 200 American companies have signed up for the Safe Harbor, including major companies that collect and use personal information such as Microsoft, Intel, and Hewlett Packard. It should also be noted that Axiom, one of the largest data collection and marketing companies in the world, has signed up for the Safe Harbor. Axiom has over 160 million names in its marketing databases.

Under the European Union Safe Harbor, companies must give notice of their data collection practices and give individual citizens in Europe an opportunity to opt-out of the use of commercial marketing of personal information. Individuals must give their prior, opt-in consent before companies can collect and use sensitive personal information relating to “racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, \* \* \* or medical or health conditions, or the sex life of the individual.” Individuals are granted a right of access to their personal information, along with the ability to correct, amend, or delete it, so long as the burden on the company is not disproportionate to the risks to the individual's privacy. Companies must also provide reasonable security to the personal information they have collected. The Safe Harbor also prohibits the onward transfer of personal information to third parties unless those parties also adhere to the Safe Harbor, to the Directive as implemented in the Member states, or to an agreement that they are providing an equivalent level of privacy protection. The Committee notes that S. 2201 would largely provide protections to U.S. citizens using the Internet that are similar to those already provided in Europe.

#### STATE LAWS ON INTERNET PRIVACY

In recent years, the 50 States have begun considering numerous bills and regulations to protect individuals' privacy, both on the Internet and off. This trend is accelerating as a few of these privacy proposals are becoming law or progressing toward enactment. Two of the more prominent recent examples include the States of Vermont and Minnesota: Vermont, which now prohibits the sharing of individuals' financial and medical information without first obtaining their prior consent (opt-in); and Minnesota, which recently enacted legislation requiring that Internet service providers obtain consent from individuals before sharing their personal information.

As momentum grows in the State legislatures and agencies across America to regulate privacy, some companies that previously opposed Federal legislation, though divided on the appropriate approach, now support a uniform standard that clearly preempts these various, inconsistent State laws.

## BACKGROUND ON THE INTERNET

The Internet represents one of the most significant technological advancements of the 20th Century. On the Internet, data about almost any subject can often be accessed in a matter of seconds. And, unlike other informational sources, the Internet is virtually unrestricted by boundaries, from a functional and economical perspective. Because of its capacity for direct communications, as well as fast, detailed data transfers, the Internet has become a highly attractive medium for commercial enterprises, marketers, and consumers. Today, consumers can avail themselves to a wide range of retail products, a variety of services, such as banking and investing, and innumerable research tools. According to marketing experts, the Internet often allows consumers to search for and purchase goods more efficiently than in the traditional, offline marketplace.

While the Internet provides these advantages, it also poses distinct risks, including a threat to the personal privacy of users. For example, the Internet provides companies a platform from which they can more efficiently monitor and track interests than is possible in the “offline,” traditional marketplace. This Internet profiling, which is achieved via the recording of “click-stream” data, often may occur without an individual’s knowledge or consent. People’s personal information that is collected and compiled may be turned into commercial profit as companies share, sell, and trade that information in the Internet marketplace, and beyond. Individuals’ personal information and Internet habits are also used to “personalize” their Internet experience, as companies analyze and utilize that information to target those individuals with a proliferation of banner advertisements, marketing pitches, discounts, and promotions. Such personalization and customization unquestionably can enhance the Internet experience of individual users, even as it simultaneously provides remunerative benefits to the corporation that practices such personalization. Indeed, the technologies used on the Internet can dramatically facilitate consumers’ experiences. These practices, however, raise privacy concerns to the extent they are occurring without the informed consent of Internet users.

It is estimated that over 105 million people in the U.S. are now using the Internet on a regular basis. According to the FTC, total online retail sales for 2000 were almost \$26 billion, and fourth quarter 2000 online retail sales were \$8.7 billion, an increase of 67 percent from the fourth quarter of 1999. According to Forrester Research, online retail sales are predicted to reach \$184 billion by 2004. Finally, Forrester Research reported that the Internet failed to realize almost \$15 billion in revenues in 1999 due to users’ concerns over threats to their privacy.

Direct marketing solicitations have been accorded constitutional protection as commercial speech and are not novel, nor are they confined to the Internet. Rather, it has been present in different forms for decades, involving methods such as door to door sales, and more modern approaches such as telemarketing and direct mail marketing (i.e. sending catalogs). The unique quality of the Internet, however, facilitates direct contact with a vast market of consumers more expeditiously and enables the collection of a far

greater catalog of information about individuals than is possible in the “offline” traditional marketplace. In the traditional marketplace, information gathering typically occurs when individuals engage in transactions that personally identifies them (e.g., purchasing an item in a store with a credit card, ordering an item from a catalogue, or subscribing to a magazine). On the Internet, however, an individual’s every step—or to be more precise, every click—may be observable, recordable, and compilable into an online profile, regardless of whether or not he or she ever engages in any commercial activity (e.g., researching stocks, looking up health information, or simply browsing for items without buying them). This is commonly referred to as “click-stream” data.

Providers of goods and services describe this distinction as an advantage that allows them to market items to consumers more personally (allowing for tailoring of services to fit consumers’ personal interest and needs), and often at a reduced cost. Moreover, they allege that the collecting and commercializing of either aggregate or specific personal information can even be the difference that maintains a website’s viability and keeps the Internet predominantly free. Some privacy advocates and academics believe that these claims, while perhaps accurate for some web operations, are exaggerated in light of analyst predictions about the Internet’s proliferation in coming years. Regardless, other economic analysis suggest that the Internet also forgoes significant revenues due to fears over personal privacy. Moreover, privacy and consumer advocates argue that these activities should only be countenanced if individuals have consented to the collection and use of their personal information.

#### PERSONAL INFORMATION COLLECTED ON THE INTERNET

Personal information collected on the Internet ranges from home telephone numbers and addresses, consumers’ names and e-mail addresses, as well as information such as social security numbers, medical records and financial data. Typically, this information is supplied by the consumer to the website during a transaction or in return for free services. Other personal information that may be collected includes buying habits, research interests, and personal lifestyle preferences (i.e. places of travel, social activities). There are several important questions that are raised with respect to personal information collected on the Internet. For example, are companies collecting more personal data than necessary for a given transaction, and is the information being sought for alternative and additional purposes? Is the personal information being safeguarded, so as to prevent access by other parties? Or, is the data being shared for internal marketing or profiling purposes, or with third parties, and if so, is such sharing done with the knowledge and consent of the individual? Finally, are entities collecting personal data directly from the individual or through other sources and means unbeknownst to the individual? It should be noted, however, that according to the most recent survey of online privacy practices, the vast majority of the most commonly visited websites now post privacy policies with respect to how they collect, use and disclose personal information.

## TECHNOLOGY USED TO COLLECT INFORMATION ON THE INTERNET

Personal information can be gathered on the Internet in a variety of ways. The simplest method utilizes collection from the individual directly. Often the consumer is asked to provide data for the purpose of completing a transaction or receiving a service. As noted above, however, even if the data is provided voluntarily, issues may subsequently arise as to whether that data is used for purposes beyond those for which the information was voluntarily granted. Online businesses can also collect data without the consumer's knowledge, by directly collecting it or by acquiring it from a third party that has already collected the information.

Personal information can be collected without the user's knowledge by technological devices commonly known as "cookies." A cookie is a text file placed on a consumer's hard drive by a company that can perform a variety of information collection functions. For example, it enables the functionality of a commercial website, such as shopping carts, wish-lists, and other features preferred by many Internet users. In addition, cookies may be used to store information about which sites the consumer has visited on the Internet. That information is then recoverable by the company that placed the cookie. This tool gives web site operators one mechanism to track consumers' online activities and gather information about their personal interests and preferences. For example, when a consumer visits a site operated by a company that placed a cookie, the company is able to identify the user in order to provide personalized features, such as e-mail for that user. Some companies may also use the identifier to keep track of the user's activities on that site. The information that is recorded may include the number of visits to a particular site and information surveyed. For those companies that use cookies in this fashion, this mechanism facilitates the compilation of profiles through click-stream data about individuals' commercial and non-commercial, and potentially sensitive, activities on the Internet.

In addition, technology known as "web bugs" is increasingly deployed by companies on the Internet including "network advertisers" (the companies that place banner advertisements on web sites) to collect information about Internet users on sites that may not even display banner advertisements. Web bugs collect information in much the same manner as do cookies, but less transparently given that a company can place them on sites on which it does not have a visible presence.

Another recent phenomenon involves the use of software installed on a user's personal computer, or downloaded by the user off the Internet to track the user's activities online. In such instances, the software has been transformed into "spyware" according to privacy advocates and is likely tracking users and compiling a personal profile of them without their knowledge or consent.

Indeed, individuals are generally unaware of the fact that a third party, such as a network advertiser, may be reaching through the website the individual has chosen to visit and collecting information about their activities. Additionally, even in situations where notices about cookies are provided to users, some websites merely inform individuals that cookies are harmless bits of data that help customize and personalize their experience. While cookies them-

selves are not bad per se, and in fact often improve a user's online experience, the use of cookies to monitor individuals' activities across multiple websites may undermine the efforts of consumers to protect their privacy.

These collection technologies can amass, in addition to personal information: the websites and web pages visited; the time and duration of the visit; subjects researched as evidenced through search terms typed in search engines, and other queries; purchases made online; "click-through" responses to advertisements; and the previous page visited by the particular individual. Once in possession of this information, businesses may develop "inferential" or "psychographic" data—information that the business infers about the individual based on the actual behavioral data that has been captured. From this amassed data, elaborate inferences may be drawn, and conclusions reached, that may or may not be accurate with respect to the individual's interests, habits, associations, and other traits.

A further concern is that even on those occasions when information about the collection practices of network advertisers is provided to individuals, this "notice" is often supplied after data collection has begun. Thus, the moment a user visits a website, multiple cookies could be placed on the user's hard drive well before there has been any chance to read a privacy policy and opt out of the collection that has already begun. However, it should be noted that many sites offer the user the ability to opt out of, and terminate, previously-collected click-stream recordings.

Although technology is used to facilitate information collection, the Committee recognizes that technology is also used to create tools for consumers to protect their personally identifiable information by allowing them to control whether, and under what circumstances, they would permit its collection, use, or disclosure. These technological tools are typically software products or online services for consumers that provide privacy protection in two general ways. One way is to prevent the collection of personally identifiable information by concealing, cloaking or decoupling the identity of the user from their online activities. Consumers are increasingly taking advantage of this kind of technology by installing software such as "personal" firewalls on their home and laptop computers to prevent harmful application downloads (like information collection devices) and other intrusions from the Internet, as well as to monitor and control the outflow to the Internet of personal information stored on their computer. Consumers also use software and online services (like Anonymizer.com) to anonymously browse websites and new payment mechanisms to purchase products and services online with cash-like anonymity.

In addition to preventing personal information collection, a second way privacy tools are used is to help consumers understand and control how their information is used or shared by the particular websites they visit. This approach takes advantage of the increasing availability of "machine-readable" privacy policies such as the Platform for Privacy Preferences (P3P) format developed by the World Wide Web Consortium. At its most basic level, P3P is a standardized set of multiple-choice questions that websites answer about their privacy policies and make available online in a computer-coded format. These answers present a snapshot of how

a website handles personal information about its users. P3P-enabled browsers, including the latest versions of both major web browsers, can “read” this coded snapshot (if available at a website) and automatically compare it to the privacy preferences set by the consumer on the browser. The browser warns consumers of any mismatch between their preferences and the websites’ policies and offers them choices on how to proceed. Proponents of P3P assert that it enhances consumer control of their personal information by putting privacy policies where users can find them and in a form users can easily understand. According to the Internet Education Foundation, P3P is the leading machine-readable privacy policy standard and has been implemented by approximately 40 of the top 100 websites, all of the top web advertisers, and several government agencies such as the FTC, the United States Department of Commerce, and the United States Postal Service.

#### PUBLIC CONCERNS ABOUT PRIVACY

Numerous studies demonstrate that the misuse of personal information that leads to a loss of privacy is the main concern Americans have about using the Internet. A Harris Interactive survey released in February 2002 listed the top three “major concerns” that consumers expressed, with respect to privacy and security on the Internet, as follows:

- companies will provide their information to other companies without their permission (75 percent);
- online transactions may not be secure (75 percent); and
- hackers could steal their personal data (69 percent).

Other analyses suggest that as many as 25 percent of all Internet users give false personal information in order to protect their identity and privacy online. In March 2000, Business Week reported that 57 percent of Americans believe that Congress should pass laws to govern how personal information is collected and used on the Internet. And, in August 2000, 86 percent of those surveyed by the Pew Research Foundation voiced their support for opt-in protection as a necessary component of any company’s privacy policy. Perhaps most surprisingly, a Harris Interactive survey commissioned by Dell and the National Consumers League reported in October 2000 that “more Americans are very concerned about their loss of personal privacy (56 percent) than health care (54 percent), crime (53 percent), and taxes (52 percent). \* \* \* When asked specifically about their online privacy,” those polled “were most worried about websites providing their personal information to others without their knowledge (64 percent) and web sites collecting information about them without their knowledge (59 percent). \* \* \* 71 percent said it is absolutely essential that companies ask consumers’ permission before using their personal information for any purpose other than the one originally given.”

It should be noted, however, that despite professing concern about online privacy, the percentage of people who bought something online during the holiday season increased from 20 percent in 1998 to 55 percent in 2000, according to the Competitive Enterprise Institute (CEI). Moreover, CEI noted that while there were 4.9 million credit card transactions online in 1997, this number had increased to 19.3 million by the third quarter of 1999.

These concerns have not abated since the tragic terrorist attacks of September 11, 2001. While Americans generally are willing to forgo some privacy to assist law enforcement efforts to monitor potential criminal and/or terrorist activities, that willingness does not translate into a desire to allow increased control over their personal information online so that companies can collect, compile, commercialize and profit from it. Some of the most prominent businesses on the Internet, including Microsoft, Intel, Hewlett Packard, eBay.com, Amazon.com, Alta Vista, Earthlink, the New York Times, and Expedia, recognize this fact and offer consumers significant privacy protections via opt-in consent regimes.

#### THE FTC AND INTERNET PRIVACY

The FTC is the Federal agency that possesses primary jurisdiction over online privacy. This jurisdiction is derived from the grant of authority to the Commission under section 5 of the Federal Trade Commission Act, which provides the FTC authority over unfair and deceptive acts and practices involving the marketing and sale of goods and services to consumers in the U.S. marketplace. According to a 2000 report by the FTC, matters concerning consumer privacy protection are best governed by core "Fair Information Practices" principles that have been in the discourse of the privacy debate for over twenty years. They are: notice, choice, access, and security.

The FTC began its review of Internet privacy issues in April 1995. Since that time, the Commission has conducted several major public workshops and hearings on the issue, including summer workshops in 1996 and 1997. Based on the information gathered through these sessions, and through independent investigations, the Commission has produced three official reports on online privacy. The first report, in 1998, recommended self-regulation as a means of achieving consumer privacy protection, while recommending legislation to protect the privacy of children's information on the Internet. The Children's Online Privacy Protection Act of 1998 (COPPA) was Congress' response to this recommendation.

That legislation was enacted within four months of introduction as part of the Omnibus Appropriations Act of 1998 [P.L. 105-277]. The Act requires companies to: (1) provide parents notice of their information practices; (2) obtain prior parental consent; (3) upon request, grant parents the option to review the information; (4) provide parents the opportunity to bar further use of information already collected; (5) limit collection of personal data on a child to participation in a game, or prize offer, and to information reasonably necessary for the activity; and (6) establish procedures to protect the security of the information. This law is in effect today and was nearly unanimously supported by the Internet industry.

In 1999, the FTC issued its second Internet privacy report and again urged industry to improve its performance in voluntarily protecting consumer privacy on the Internet. The FTC again called for self-regulation generally, but cautioned that if industry did not dramatically improve upon its performance, the Commission may recommend Internet privacy legislation in the future. In May 2000, the FTC released its third report on online privacy. For the first time, the Commission concluded that self-regulation alone is not sufficient to ensure adequate consumer privacy protection and

called for legislation that would codify the core “Fair Information Practices.” Specifically, the FTC found that only 20 percent of a random sample of major commercial websites have implemented all four fair information practices of notice, choice, access, and security. And, even among the 100 most popular U.S. commercial websites, only 42 percent had implemented these principles. The vote in favor of this recommendation was 3–2. Commissioner Leary concurred in part and dissented in part (recommending, among other things, more narrow legislation that only requires notice but that covers the online and offline marketplace). Commissioner Swindle dissented on grounds that evidence existed showing consumers were increasingly protected by industry self-regulatory efforts and this process should not be inhibited prematurely by regulation.

More recent figures obtained using the FTC’s survey methodology show significant improvement since the FTC’s report two years ago. A report of the Progress & Freedom Foundation, released in March 2002, indicates that websites are collecting less information (96 percent to 84 percent), using fewer third-party cookies (78 percent to 48 percent), providing more prominent and complete notices, providing consumers with more choice in the use of personally identifiable information (77 percent to 93 percent), increasingly offering opt-in as opposed to opt-out, and increasingly offering a combination of fair information practice elements. Most importantly, it found that 99 percent of the 85 busiest websites had posted privacy policies, and 80 percent of a random sample of websites had done so as well. In fact, many prominent Internet industry witnesses testified that their companies would already be in compliance with this, or similar, legislation.

The 2000 FTC recommendation suggested setting forth: “a basic level of privacy protection for consumer-oriented commercial websites. \* \* \* Consumer-oriented commercial websites that collect personal identifying information from or about consumers online would be required to comply with the four fair information practices by providing individuals: (1) clear and conspicuous notice of their information practices; (2) an ability to choose not to have their personal information collected and used as described in that notice; (3) reasonable access to information collected, including an opportunity to correct or delete the information; and (4) reasonable security to protect the information collected.”

While these were the legislative standards the FTC recommended under former Chairman Pitofsky in its May 2000 report to Congress, these broad definitions would require extensive FTC clarification in a rulemaking. The FTC has considerable experience in this complex area. For example, while the FTC’s Advisory Committee on Access and Security acknowledged, in an internal report, that it could not reach a consensus on the extent to which access and security requirements could or should be implemented, in 2000, the FTC successfully implemented COPPA, and in the process imposed reasonable access and security requirements on websites collecting personal information from children online.

Following this recommendation, in July 2000, the FTC concluded its two year survey of the Internet network advertising industry (comprised of the companies that place “banner advertisements” on Internet sites). In doing so, the FTC reached a settlement agreement with approximately 90 percent of the current members of the

network advertising industry. In that agreement, the network advertisers agreed to provide notice of their profiling activities on the Internet.

Since the present Bush administration took office, the FTC has departed from its pro-legislation stance. While Commissioners Thompson and Anthony are on record supporting varying degrees of legislation, FTC Chairman Muris and Commissioner Swindle have publicly stated their opposition to legislation at this time, preferring to focus on increased enforcement of existing law. In a speech on October 4, 2001, Chairman Muris laid out his view that: "It is too soon to conclude that we can fashion workable legislation to accomplish [online privacy legislation's stated] goals. We need to develop better information about how such legislation would work and the costs and benefits it would generate. \* \* \* I think there is a great deal we can do under existing laws to protect consumer privacy. \* \* \* At this time we need more law enforcement, not more laws."

In letters dated April 24, 2002, each of the five FTC Commissioners responded to an inquiry by Senator McCain asking whether they believed privacy legislation was needed, and if so, what it should contain. Senator McCain's inquiry also requested their comments on the principal features of S. 2201. The Commissioners' response letters were introduced into the record at the April 25 hearing on the bill. Two of the five Commissioners believe that legislation is needed at this time and are supportive of the bill. Three Commissioners, including Chairman Muris, express strong reservations about the workability of the provisions of S. 2201 and whether any legislation is needed in light of existing privacy law, increased FTC enforcement, and industry efforts to improve protections.

Although the Commissioners were not asked the question specifically, each of their responses addressed the issue of whether privacy legislation should apply only to *online* businesses and information practices, or to both the *online* and *offline* worlds equally. Four of the five Commissioners concluded that any legislation addressing privacy should not draw differences between online and offline privacy protections. The majority of the Committee believes that S. 2201, as reported, responds to and addresses this fundamental concern raised by the FTC.

#### POSITIONS OF CONSUMER PRIVACY ADVOCATES AS TO NEED FOR LEGISLATION

The primary consumer privacy advocacy groups include the Consumers Union, the Center for Democracy and Technology, the Electronic Privacy Information Center, and the Consumer Federation of America. These groups support the contention that legislation is needed to protect individuals' privacy on the Internet. These groups argue that not all industry policies are complete or reliable, which they assert is proven by recent surveys and by a sampling of many online privacy policies. Those consumer groups acknowledge that there are effective self-regulatory efforts but believe those efforts are not sufficient to prevent bad actors. Some of these groups also argue that official uniform rules are needed to ensure industry compliance with a core set of Fair Information Practices, which can only be accomplished through legislation.

## LEGISLATIVE HISTORY

Senator Hollings introduced S. 2201, the “Online Personal Privacy Act,” on April 18, 2002. The legislation was referred to the Commerce Committee. The bill was originally cosponsored by Senators Stevens, Inouye, Burns, Rockefeller, Kerry, Breaux, Cleland, Carnahan, and Nelson. Senator Torricelli was subsequently added as a cosponsor. This legislation represented a compromised approach between three bills considered by the Commerce Committee during the 106th Congress: S. 809, introduced on April 15, 1999, by Senator Burns, and cosponsored by Senators Wyden and Kohl; S. 2606, introduced on May 23, 2000, by Senator Hollings, and cosponsored by Senators Inouye, Rockefeller, Breaux, Bryan, Cleland, Byrd, Kerrey, Edwards, Feingold and Durbin; and S. 2928, introduced on July 26, 2000, by Senator McCain and cosponsored by Senators Abraham, Kerry and Boxer. The Commerce Committee also held four hearings on the issue of Internet privacy in the 106th Congress to examine the issue generally, as well as the three bills referenced above. None of these bills were reported out of Committee.

On April 25, 2002, the Committee held a full Committee hearing on S. 2201. Testimony was provided at the hearing by: Marc Rotenburg of the Electronic Privacy Information Center; Paul Misener, Vice President of Global Public Policy, Amazon.Com; Barbara Lawler, the Chief Privacy Officer of Hewlett-Packard; Frank Torres, of the Consumers Union; and John Dugan, a law partner at Covington and Burling who testified on behalf of the Financial Services Coordinating Council, the association representing companies in the diversified financial services industry. The Committee also received written testimony from a number of other interested industry parties, academics, consumer advocates, and the individual commissioners at the FTC.

On May 17, 2002, the Committee ordered S. 2201 to be reported favorably with an amendment in the nature of a substitute, and three amendments thereto. The substitute amendment was offered by the Chairman and contained the following major changes: (i) incorporation of offline privacy provisions requiring the FTC to recommend offline regulations and then implement those regulations if Congress fails to act to require a different approach; (ii) incorporation of a safe harbor program to facilitate compliance and enforcement of the legislation’s requirements with respect to operators and provide an affirmative defense for operators in private litigation brought pursuant to the legislation; and (iii) a revised right of action that provided for statutory damages only in the event of violations involving sensitive personal information and either fraudulent notice or disclosure of such information. Other clarifying changes were included in the substitute amendment (some of which are described below in the section-by-section analysis) to more accurately reflect the intent of the legislation as introduced, and reconcile the legislation with some existing privacy statutes to generally preserve their existing pro-consumer privacy protections.

Two amendments were adopted to the substitute by voice votes and one by unanimous consent. An amendment by Senator Brownback was adopted to exempt from the legislation small businesses that do not share personally identifiable information or

process such information. An amendment by Senator Nelson was adopted that required operators covered by the legislation to designate a privacy compliance officer. And an amendment by Senator Allen was adopted, as amended by Senator Hollings, to clarify that reasonable access requests by users should take into account the need by operators to protect proprietary information associated with the personal information they possess about users.

Several amendments were defeated by roll call votes.

Senator McCain offered an amendment to ensure that equal obligations were imposed on the collection, use and disclosure of personally identifiable information both online and offline. This online-offline amendment failed by a vote of 14–9. Specifically, the amendment would have added a new section to S. 2201 to clarify that nothing in the legislation could be construed to impose different standards of care or obligations on the collection, use or disclosure of personally identifiable information online than were imposed offline. In order to ensure that Federal regulations promulgated under the legislation would meet this principle, the McCain amendment would have suspended enforcement of the bill until online and offline privacy regulations were imposed equally on all persons. This amendment could have potentially postponed the implementation and enforcement of the legislation indefinitely because it might never be achievable for the FTC to implement regulations covering both online and offline privacy to the exact equivalent extent that would have been required by the legislation had the McCain amendment passed.

An amendment offered by Senator Brownback that would have set forth specific criteria by which operators could satisfy the reasonable security requirements of title I failed by a vote of 14–9. Senator Brownback’s amendment would have set out parameters for companies to follow so that their security procedures would be deemed to satisfy the bill’s requirement of reasonable security, “without regard to whether such procedures have prevented a breach of network security.”

An amendment offered by Senator Allen that would have broadened the preemption provision in the legislation to preempt State common law failed by a vote of 14–9. This amendment would have eliminated common law rights of action for individuals aggrieved by violations of the legislation where the private right of action in the legislation would not provide for recovery.

A second amendment offered by Senator Allen to eliminate the private right of action failed by a vote of 15–8. The Committee notes that the legislation only provides a private right of action for individuals aggrieved by violations involving their sensitive personally identifiable information in the cases of disclosure of that information and/or fraudulent notice by operators.

A third amendment offered by Senator Allen that would have provided operators in compliance with any of 17 other Federal privacy laws a safe harbor from inconsistent provisions of S. 2201 failed by a vote of 14–8.

#### SUMMARY OF MAJOR PROVISIONS

S. 2201 would provide a comprehensive approach to protecting privacy on the Internet. The bill’s approach would apply a core set of Fair Information Practices principles which have been in the

public discourse about privacy for the better part of three decades. These principles require a baseline of privacy protection that includes providing individuals rights of notice, consent, access, security and enforcement. The legislation also would provide broad preemption of State statutes, rules, or regulations that relate to the collection, use, or disclosure of personally identifiable information obtained through the Internet.

Title I of the legislation would set forth the rules governing the collection and use of individuals' personally identifiable information gathered online. These rules would apply to Internet service providers, online service providers or operators of commercial websites (hereinafter collectively referred to as "operators"), in addition to third parties using such operators to collect information about users of an Internet service or website. Specifically, the rules would require operators to provide clear and conspicuous notice of their collection and use practices with respect to personally identifiable information. If the personally identifiable information collected about the user is sensitive, operators may not collect or use that information without first, or contemporaneously, gaining the user's affirmative, opt-in consent. If the personally identifiable information collected about the user is not sensitive, operators may not collect or use that information without first, or contemporaneously, affording users robust notice of the intent to use the information, and giving the user the opportunity to decline consent via an opt-out mechanism. In addition, title I would require operators to notify users if they make material changes in their privacy policies or if their policy has been breached.

Title I also would provide for significant exceptions to the legislation's notice and consent requirements in several instances: (1) to protect the security or integrity of the service or website, or ensure the safety, health, or life of other people or property; (2) to conduct a transaction, deliver a product or service, complete an arrangement for which the user provided the information, or provide products, services, or conduct activities integrally related to the transaction, product, service, or arrangement sought by the user; and (3) to comply with some of the Fair Credit Reporting Act's non-marketing related provisions. Other exceptions include appropriate disclosures to law enforcement entities, in court proceedings, for emergency purposes to professional services providers, and for some non-marketing business activities permitted for financial institutions under the Financial Services Modernization Act.

Finally, title I would require operators to grant users reasonable access to their information once collected, and provide users reasonable security for that information once collected. The reasonableness of an access request shall be based on balancing factors such as the sensitivity of the information requested and the burden on the operator of complying with the request. Operators would be permitted to charge a small fee for such access not to exceed three dollars.

Title II would set forth the enforcement provisions in the legislation, and generally allow enforcement by the FTC, the State attorneys general, and individual rights of action. First, it clarifies that any violation of title I is an unfair or deceptive act or practice proscribed by section 5 of the Federal Trade Commission Act. To the extent that operators covered by the legislation are more typically

regulated by entities other than the FTC, title II grants those other Federal authorities exclusive authority to enforce title I as to those operators. To the extent a civil penalty is imposed on an operator due to a violation of title I with respect to non-sensitive personally identifiable information, the FTC is authorized to hold the penalty in trust for distribution to users aggrieved by the violation. Such payment could not exceed \$200 per user. This title also preserves the application of section 222 of the Communications Act of 1934, and clarifies that operators providing Internet services over cable facilities are governed by this legislation with respect to such services, rather than by the Cable Act of 1984. The legislation would permit a State attorney general to bring a civil action as *parens patriae* to enforce a violation of the legislation on behalf of residents of the State in a district court.

Title II would also create a process for the establishment of safe harbor self-regulatory programs to provide operators with some predictability as to their compliance with the requirements of the legislation. The safe harbor provision permits self-regulatory organizations and independent third party verifiers to certify that operators are in compliance with the Act. Such certifying entities will oversee companies' compliance with the legislation, conduct random audits of those companies, and alert the FTC of any non-compliance. In addition, any company that is a member of a safe harbor program will be entitled to an affirmative defense in a private right of action permitted by this Act that is brought by individuals aggrieved by a violation of the Act. A safe harbor will augment FTC enforcement by enabling additional oversight of companies subject to the requirements of the Act, while providing companies greater certainty that their practices and procedures are in fact compliant. A broader safe harbor is included for small businesses, who are exempted from the requirements of the legislation if they meet certain size requirements and do not process personally identifiable information of consumers or disclose such information for consideration to others.

Title II would also create a private right of action for users to enforce violations of title I involving sensitive personally identifiable information. With respect to violations involving fraudulent notice or disclosure associated with sensitive personally identifiable information, aggrieved individuals may bring an action in an appropriate court in a State to enjoin the violation, recover actual monetary loss from the violation, or receive up to \$500 in statutory damages, whichever is greater, or both actions. With respect to other violations of title I involving sensitive personally identifiable information, aggrieved individuals may bring an action in an appropriate court in a State to enjoin the violation or recover actual monetary loss from the violation, or both actions. In any right of action brought by individuals under this legislation against operators, defendants would have an affirmative defense if they have established and implemented with due care reasonable practices and procedures to ensure compliance and are deemed to be in compliance by a self-regulatory organization or certified independent verification organization pursuant to the safe harbor provision referenced above.

Finally, title II would provide for whistleblower protection for employees who notify Federal enforcement agencies or State attorneys general as to violations of title I of the legislation.

Title III would apply the legislation to Federal agencies and requires the Senate Sergeant at Arms to develop regulations setting forth a privacy policy for U.S. Senate offices.

Title IV contains miscellaneous provisions for the legislation. A provision on definitions defines pertinent terms for the legislation as described more fully in the section-by-section analysis below. A provision requires the FTC to initiate and complete a rulemaking for regulations to implement title I within one year of enactment. A provision establishes an effective date for the legislation one day after publication of the FTC's final rule. And a provision requires the FTC to report to Congress 18 months after enactment, and annually thereafter as to: whether the Act is accomplishing its intended purposes; whether pro-privacy technology is being used in the marketplace to facilitate compliance; whether additional legislation is needed; and whether the government can facilitate the development of standard online privacy notices. Finally, title IV would require the National Institute of Standards and Technology to encourage technologies such as P3P for protecting privacy online.

Title V would require the FTC to submit recommendations to Congress within 6 months of enactment as to proposed regulations on offline privacy that would provide individuals a level of protection similar to that provided by this legislation for online privacy. If Congress does not enact legislation within 12 months of receipt of the FTC proposed offline rules, then the FTC is directed to promulgate those rules within one month of Congress failing to act.

#### ESTIMATED COSTS

In accordance with paragraph 11(a) of rule XXVI of the Standing Rules of the Senate and section 403 of the Congressional Budget Act of 1974, the Committee provides the following cost estimate, prepared by the Congressional Budget Office:

U.S. CONGRESS,  
CONGRESSIONAL BUDGET OFFICE,  
*Washington, DC, June 18, 2002.*

Hon. ERNEST F. HOLLINGS,  
*Chairman, Committee on Commerce, Science, and Transportation,  
U.S. Senate, Washington, DC.*

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for S. 2201, the Online Personal Privacy Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Ken Johnson (for federal costs), Angela Seitz (for the state and local impact), and Nathan Musick (for the private-sector impact).

Sincerely,

BARRY B. ANDERSON  
(For Dan L. Crippen, Director).

Enclosure.

## CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

*S. 2201—Online Personal Privacy Act*

Summary: S. 2201 would impose several restrictions on the collection of personal information over the Internet. For example, Internet service providers, online service providers, and operators of commercial websites would be required to obtain users' consent before collecting sensitive data and provide users the opportunity to "opt out" before gathering nonsensitive data. Also, under the bill, the Federal Trade Commission (FTC) would propose and implement similar restrictions on the collection of personal information by means other than the Internet. Finally, the National Institute of Standards and Technology (NIST) would be required to support the development of new software that gives Internet users automatic access only to websites with the users' preferred policies on privacy.

The restrictions on collecting personal information contained in S. 2201 would be enforced primarily by the FTC. However, agencies such as the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation (FDIC), the Office of Thrift Supervision (OTS), the National Credit Union Administration (NCUA), the Securities and Exchange Commission (SEC), and the Secretary of Transportation would enforce the bill as it applies to the agencies' respective jurisdictions. These agencies would punish violations with civil and criminal penalties. Under the bill, any civil penalties collected by the FTC would be distributed to the victims of the violations.

Assuming appropriation of the necessary amounts, CBO estimates that implementing this bill would cost the FTC \$9 million and NIST \$11 million over the 2003–2007 period. Because S. 2201 would create new civil and criminal penalties and would impose costs on federal banking regulators, we also estimate that the bill would have negligible effects on both direct spending and revenues. Therefore, pay-as-you-go procedures would apply.

S. 2201 would impose intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA). CBO cannot determine whether the costs of complying with some of these mandates would exceed the threshold established in UMRA (\$58 million 2002, adjusted annually for inflation).

S. 2201 also contains private-sector mandates as defined in UMRA. CBO cannot determine whether the direct cost of those mandates would exceed the annual threshold set by UMRA for private-sector mandates (\$115 million in 2002, adjusted annually for inflation). The mandate costs are difficult to estimate because of uncertainties about (1) the number of online firms affected by S. 2201, (2) the incremental costs the bill would impose on any of those firms in light of existing privacy statutes, and (3) how the Federal Trade Commission would implement certain of the requirements of S. 2201 with regard to online and offline personal privacy.

Estimated cost to the Federal Government: The estimated budgetary impact of S. 2201 is shown in the following table. The costs of this legislation fall within budget function 370 (commerce and housing credit).

	By fiscal year, in millions of dollars—				
	2003	2004	2005	2006	2007
CHANGES IN SPENDING SUBJECT TO APPROPRIATION					
FTC spending to enforce privacy restrictions: <sup>1</sup>					
Estimated authorization level .....	1	2	2	2	2
Estimated Outlays .....	1	2	2	2	2
NIST spending to develop internet software: <sup>2</sup>					
Estimated authorization level .....	3	2	2	2	2
Estimated outlays .....	3	2	2	2	2
Total changes:					
Estimated authorization level .....	4	4	4	4	4
Estimated outlays .....	4	4	4	4	4

<sup>1</sup>The FTC received a gross 2002 appropriation of \$156 million. This amount will be offset by an estimated \$108 million in fees the FTC collects for merger reviews.

<sup>2</sup>NIST received a total appropriation of \$680 million in 2002.

### *Basis of estimate*

Subject to the availability of appropriated funds, CBO estimates that implementing S. 2201 would cost the FTC and NIST a total of \$20 million over the 2003–2007 period. We also estimate that the bill would have an insignificant effect on direct spending and revenues. For this estimate, CBO assumes that the bill will be enacted by the end of fiscal year 2002 and that funds will be appropriated near the beginning of each fiscal year.

#### *Spending subject to appropriation*

S. 2201 would require the FTC to develop and enforce new regulations on the collection of personal information through the Internet. The bill also would require the FTC to draft regulations concerning the privacy of information collected by entities by means other than the Internet. In the absence of additional legislation, the FTC would implement those regulations 19 months after enactment. Finally, the agency would distribute any civil penalties collected for violations of the bill's provisions to the victims of those violations. Based on information from the FTC, CBO estimates that implementing the bill would require the agency to hire about 20 additional staff that would cost about \$2 million a year, subject to the availability of appropriated funds. (First-year costs—in 2003—are likely to be about \$1 million.)

S. 2201 also would require NIST to undertake efforts to promote and develop software that would enable Internet users to access only those websites that employ the users' preferred privacy policies. CBO expects that the agency would fulfill this requirement research and testing on such software and the development of relevant standards. Based on information for NIST, CBO estimates that the new personal and equipment needed to undertake these activities would cost about \$2 million a year over the 2003–2007 period, assuming the appropriation of the necessary amounts. (We estimate costs of \$3 million for 2003 because the agency would need to acquire new computers and testing equipment.)

#### *Direct spending and revenues*

The OCC, NCUA, OTS, FDIC, and the Board of Governors of the Federal Reserve System would enforce the provisions of S. 2201 as they apply to financial institutions. The OCC, NCUA, and OTS charge fees to the institutions they regulate to cover all of their administrative costs; therefore, any additional spending by these

agencies to implement the bill would have no net budgetary effect. That is not the case with the FDIC, however, which uses insurance premiums paid by all banks to cover the expenses it incurs to supervise state-chartered banks. The bill's requirement that the FDIC oversee financial institutions' collection of personal information through the Internet would cause a small increase in FDIC spending, but would not affect its premium income. In total, CBO estimates that S. 2201 would increase net direct spending of the OCC, NCUA, OTS, and FDIC by less than \$500,000 a year.

Budgetary effects on the Federal Reserve are recorded as changes in revenues (governmental receipts). Based on information from the Federal Reserve, CBO estimates that enacting S. 2201 would reduce such revenues by less than \$500,000 a year.

Because those who violate the provisions of S. 2201 could be subject to civil and criminal fines, the federal government might collect additional fines if the bill is enacted. Collections of civil and criminal penalties are classified in the budget as revenues. However, based on information from the FTC, CBO estimates that any such increase in collections would be less than \$500,000 per year.

Under the bill, any civil penalties collected by the FTC for violations of the bill's provisions would be distributed to victims of the violations. In addition, collections of criminal fines are deposited in the Crime Victims Fund and spent in subsequent years. Because any increase in direct spending would equal the amount of fines collected (with some lag), the net impact on spending also would be negligible.

Pay-as-you-go considerations: The Balanced Budget and Emergency Deficit Control Act sets up pay-as-you-go procedures for legislation affecting direct spending or receipts. Although S. 2201 would affect both direct spending and receipts, CBO estimates that the net effects would be insignificant.

Estimated impact on state, local, and tribal governments: S. 2201 would preempt certain state laws regulating Internet privacy and disclosure, thus imposing an intergovernmental mandate as defined in UMRA. The cost of the preemption would not be significant. To the extent that public entities fall under the definition of online service providers (to be defined by the Federal Trade Commission), the requirements of this bill regarding the collection, use, and disclosure of certain information also would constitute mandates, but CBO cannot determine whether the cost of complying with the collection, use, and disclosure requirements would exceed the intergovernmental mandates threshold established in UMRA (\$58 million in 2002, adjusted annually for inflation). It is difficult to estimate these costs because uncertainties in determining the total number of public entities that would be affected.

In addition, because of the wide range of existing practices regarding the collection of personally identifiable information, we cannot establish a reliable baseline of costs currently being incurred. Some states have a number of protections already in place, but other public online services have less-developed privacy policies and practices. Finally, we cannot predict how the legislation would be interpreted by the Federal Trade Commission (or in future legislation by the Congress) for both online and offline personally identifiable information collection, use, and disclosure.

Estimated impact on the private sector: S. 2201 would impose several mandates on the private sector. The bill would require Internet service providers, online service providers and other parties (e.g., operators of a website or online advertisers) to comply with a variety of privacy and disclosure requirements for personal information that they collect online and that allows them to identify individuals (defined in S. 2201 as “Personally Identifiable Information”). In particular, S. 2201 would require such businesses to:

- Provide notice to users, either before or at the point of information collection online, of the types of personal information being collected, and of the subsequent use and disclosure that will be made of that information;
- Provide users a choice of whether to allow collection of their personal information, by enabling them to opt-out from the collection of nonsensitive personal information and opt-in to the collection of sensitive personal information;
- Update users and allow for their consent whenever personal information is collected or disclosed under a “materially different” policy from that previously in effect, or notify all users when privacy has been compromised by an unintentional act of the information collector, (e.g., by a system malfunction or security breach);
- Designate a privacy compliance officer responsible for insuring that online collection and disclosure policies satisfy the requirements of the bill;
- Provide users with “reasonable” access to their personal information and allow them to make changes and deletions;
- Ensure the security of collected personal information; and
- Provide whistle-blower protection to employees who notify federal or state agencies of violations of the bill’s requirements.

S. 2201 would further require the Federal Trade Commission to promulgate regulations for offline personal information, if the Congress does not pass legislation regulating offline personal information collection and disclosure which is similar in intent and scope to the online provisions in S. 2201 within 18 months of enactment.

CBO cannot determine whether the direct costs of those mandates would exceed the annual threshold established in UMRA for private-sector mandates (\$115 million in 2002, adjusted annually for inflation). The mandate costs are difficult to estimate because of uncertainties about (1) the number of online firms affected by S. 2201, (2) the incremental costs the bill would impose on any of those firms in light of existing privacy statutes including the loss in revenue, if any, that would result from not being able subsequently to use or sell certain personal information; and (3) how the Federal Trade Commission would implement certain of the requirements of S. 2201 with regard to online and offline personal privacy.

Estimate prepared by: Federal costs: Ken Johnson; impact on state, local, and tribal governments: Angela Seitz; impact on the private sector: Nathan Musick.

Estimate approved by: Peter H. Fontaine, Deputy Assistant Director for Budget Analysis.

## REGULATORY IMPACT STATEMENT

In accordance with paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee provides the following evaluation of the regulatory impact of the legislation, as reported:

## NUMBER OF PERSONS COVERED

S. 2201 would provide privacy protections for all individuals using the Internet, and ultimately, for all individuals engaging in the traditional, offline marketplace. As such, the legislation would cover potentially all consumers and those engaged online, as well as offline, and those companies that operate in either or both spaces.

## ECONOMIC IMPACT

This legislation would result in new or incremental costs for companies to comply with its privacy protection requirements to the extent they are not already doing so. Numerous studies have estimated the cost of online privacy legislation, claiming anywhere from several to tens of billions of dollars in added costs to companies for compliance with such legislation. The Committee also heard testimony from several witnesses indicating that they already were in compliance with the proposed provisions of this legislation, or with similar requirements. While these cost studies have not specifically examined the cost of offline privacy legislation similar to the offline provisions in this bill, critics of these cost analyses generally argue that they often do not take into account the fact that some of these added costs have already been borne by companies' previous compliance with existing online and offline privacy legislation.

## PRIVACY

The legislation would increase the personal privacy of all individuals who use the Internet and would not have an adverse impact on individual users.

## PAPERWORK

S. 2201 would require the FTC to perform two rulemaking procedures in order to implement the legislation, as well as to report to Congress on a regular basis about several privacy issues. As such, the legislation should generate similar amounts of administrative paperwork to legislation requiring multiple agency rulemakings and a report to Congress.

## SECTION-BY-SECTION ANALYSIS

*Section 1. Short Title*

This Act may be cited as the "Online Personal Privacy Act."

*Section 2. Table of Contents*

This section provides a table of contents for the bill.

*Section 3. Findings*

This section cites findings by Congress concerning the need for Federal Internet privacy legislation to protect privacy, boost con-

sumer confidence and e-commerce, and provide business certainty through broad preemption.

*Section 4. Preemption of State Law or Regulations*

This section states that the legislation supersedes any State statute, regulation or rule regulating Internet privacy to the extent that it relates to the collection, use, or disclosure of personally identifiable information obtained through the Internet.

TITLE I—ONLINE PRIVACY PROTECTION

*Section 101. Collection, Use or Disclosure of Personally Identifiable Information*

This section would require that an Internet service provider, online service provider or commercial website operator (hereinafter collectively referred to as “operators”) may not collect, use, or disclose personally identifiable information except in accordance with the provisions of this legislation. This requirement also applies to any third party, including advertising networks, that use an operator to collect information about users of that operator’s service or website. Examples of such third parties would include entities that make publicly available computer software that collects personally identifiable information about users and discloses that information to any person other than the user, as well as companies that provide outsourced website hosting or other technical services to maintain online operations for an operator that collects or uses personally identifiable information in the course of their business.

*Section 102. Notice and Consent Requirements*

This section would require operators that collect personally identifiable information to provide users clear and conspicuous notice as to the specific types of personally identifiable information to be collected, the methods of collecting and using the information collected, and all disclosure practices for that information (including whether it will be disclosed to third parties). The notice requirement imposed by this section is not required with respect to personally identifiable information collected by the operator prior to the effective date of the legislation, except to the extent such information is combined with personally identifiable information collected after the effective date, at which point it would come under the notice requirements of the legislation. Under such a circumstance, notice of this combination would only be required at the initial point of collection of personally identifiable information after the effective date of the legislation. For example, a statement in the privacy policy by an operator after the effective date of the legislation that “we may combine your information with information collected previously,” would suffice. Regardless, the Committee does not intend that notice would ever be required prior to the effective date. The Committee contemplates that the FTC, in interpreting term “clear and conspicuous notice”, should be guided to the extent practicable by the meaning embodied in the FTC’s implementation of COPPA, which required children’s websites to provide parents clear and conspicuous notice of their information collection practices with respect to children’s information. In other words, a link to a privacy policy, prominently displayed would con-

stitute clear and conspicuous notice. In turn, that policy would have to meet the specific requirements of this section as to the types of information collected, the methods of collecting and using the information, and the disclosure practices intended for the information.

Under section 102(b), an operator may not: (1) collect sensitive personally identifiable information, as defined by this legislation, online; or (2) disclose or otherwise use such information collected online, unless the operator obtains that user's consent to the collection and disclosure or use of that information before, or at the time, the information is collected, and that consent is evidenced by an affirmative act in a written or electronic communication.

Under section 102(c), an operator may not: (1) collect personally identifiable information that is not sensitive online; nor (2) disclose or otherwise use such information collected online from a user, unless the operator provides robust notice as defined by this legislation to the user in addition to clear and conspicuous notice, and has given the user an opportunity to decline consent for such collection and use before, or at the time, the information is collected. Under section 102(d), robust notice is only required by a provider upon its first collection of non-sensitive personally identifiable information from a user, provided that a subsequent collection of materially different non-sensitive information would also require robust notice. The term "materially different" information would include materially new or user-revised information as to a person's name, address, phone number, e-mail address, or birth certificate number, but would not include additional information such as that collected via a user's click stream activity. "Materially different" information also would not include non-personally identifiable information that is subsequently combined with collected non-sensitive personally identifiable information.

The Committee notes that complying with some of the bill's privacy protection requirements presents challenges for wireless Internet service providers that their wired counterparts do not face. In particular, the spatial and functional limitations of handheld wireless devices make it more difficult for wireless Internet service providers to comply with the notice, consent, access, and other obligations imposed by the bill. The Committee expects the FTC to take into account these limitations and reflect them, as appropriate, in the regulations it adopts to implement the bill.

Under section 102(e) the consent or denial of consent by a user of permission to an operator to collect, disclose, or otherwise use information about that user for which consent is required under this Act shall remain in effect until changed by the user and shall apply to commercial or legal successors to the operator, without regard to the legal form in which such succession occurred, including successor entities that collect, use, or disclose such information as a result of a chapter 7 or chapter 11 bankruptcy proceeding under title 11 of the United States Code. The permanence of a user's consent or denial of consent does not apply if: (1) the kind of information collected by the successor entity about the user is materially different from the information collected by the predecessor entity; (2) the methods of collecting and using the information employed by the successor entity are materially different from the methods employed by the predecessor entity; or (3) the disclosure practices

of the successor entity are materially different from the practices of the predecessor entity.

*Section 103. Policy Changes; Breach of Privacy*

Section 103(a) provides that operators who materially change their privacy policies must provide notice to all users of that material change and may not collect, disclose or use personally identifiable information in accordance with the changed policy unless the user has been afforded an opportunity to consent or withhold consent, depending on the sensitivity of the personally identifiable information in question. This section is intended to require that an operator act in good faith and take reasonable measures to provide notice to users of a material policy change by, for example, electronic or postal communications. The section is not intended to require an operator to find each of its users or even research to confirm the accuracy of each user's address or receipt of the notice of policy change.

Under section 103(b), operators must provide notice of a privacy breach to users relating to those users' personally identifiable information. A breach includes disclosure of such information by an operator in violation of the legislation or the compromise of security, confidentiality, or integrity of such information by a hacker or third party. The notice provided must describe the nature of the privacy breach committed and the steps taken by the operator to remedy it. Such notice may be delayed for a reasonable period of time if postponement would facilitate: (1) the detection of a person responsible for the privacy breach (such as a hacker); and (2) restoring the integrity of the service and preventing further compromise of the security confidentiality and integrity of such information. Similarly, notice may be delayed for a reasonable period of time so as to restore the functionality of a service after a system failure and to take steps to restore the integrity of the service or website and prevent any further compromise of the security, confidentiality, or integrity of personal information due to that system failure or related incidents.

Section 103(c) requires that every operator covered by the legislation designate a privacy compliance officer responsible for ensuring compliance with the requirements of this legislation as well as the privacy policies of the operator for which they work.

*Section 104. Exceptions*

Under section 104(a), the notice and consent requirements of section 102 generally do not apply to collection, disclosure, or use by an operator of information about a user when the collection, disclosure, or use is necessary to fulfill the request sought by the user. If, however, the information is then used or disclosed for unrelated, or previously un-noticed, purposes, such as for marketing, the exemption from section 102 notice and consent requirements is no longer applicable. The Committee intends for the exception to operate so that an operator is implicitly permitted in all instances to share a user's personally identifiable information in order to fulfill a user's request.

To protect the security of the service or safety of people or property, section 104(a) provides that the notice and consent requirements under section 102 do not apply to information collected, dis-

closed, or used to: (1) protect the security or integrity of the service or website; or (2) ensure the safety, health, or life of other people or property. For example, if use or disclosure of personal information could thwart an attempt to hack the security of a website and obtain personal information about users, an operator would not have to provide notice or provide a consent mechanism with respect to such use or disclosure to the hacker under surveillance. Similarly, if collection, disclosure or use of personal information would ensure the safety of people or property by averting harm, an operator would be excused from the notice and consent requirements of this section with respect to that information.

To fulfill the purposes for which the user provided the information, there would be no notice and consent requirements in instances in which the operator's collection, use, or disclosure of personally identifiable information is necessary to conduct a transaction, deliver a product or service, or complete an arrangement for which the user provided the information. For example, if a user purchases a book from Amazon.com, his or her personal information necessarily may need to be used and disclosed to a party responsible for delivering the book to the user. No notice or consent would need to accompany this use. If, however, the information were also to be used for unrelated marketing or other purposes, Amazon.com would be required to provide notice and seek opt-out consent as required by section 102 with respect to that information. With respect to onward transfer of information that is only described by the operator for the purposes of completing the user's request, the Committee contemplates recipients of that information, such as United Parcel Service, in the Amazon.com example, will only use the personally identifiable information for purposes related to the user's request (i.e. delivery).

The Committee is aware that businesses subject to the bill may operate websites with partners as co-branded sites or may offer the products or services of others on their websites or other online media. In such instances, personally identifiable information may need to be shared between partners in order to complete the transaction, and for related purposes. Section 104 would allow the sharing of information for these purposes, absent compliance with any notice or consent requirements of section 102.

The exceptions in this section apply to information without regard to its sensitivity. If a user applies for a loan online, the lender by necessity must share sensitive personally identifiable financial information about the user with several parties, for example, to facilitate the loan request, to check on the creditworthiness of the applicant, to contract underwriters, and to ensure the identity of the applicant. Such sharing is entirely appropriate and in fact necessary for the transaction to proceed and is accordingly exempt from the notice and consent requirements of the legislation, so long as those uses of the personal information are limited to those necessary to further the user's request—in this case for a loan. Similarly, if a user seeks medical attention online and the operator provides service such as, but not limited to, treatment, recommendations, referrals, or prescriptions, any sharing of the user's sensitive personally identifiable health or medical information is permitted for these and related purposes without triggering the legislation's notice and consent requirements.

To provide other products and services or conduct activities integrally related to the purposes for which the user provided the information, section 104(a) also exempts the collection, use, or disclosure of information from the notice and consent requirements of section 102 when necessary to provide other products and services or conduct activities integrally related to the transaction, service, product, or arrangement for which the user provided the information. This exemption should be read expansively rather than in a limited fashion. For example, if a user seeks medical attention online and seeks a desired course of treatment, but is ultimately offered an unanticipated alternative course of treatment, the sharing of sensitive personally identifiable health information for the purpose of providing that treatment would be permitted even though the user did not specifically request such alternative treatment at the outset. Or, if a person applies for a mortgage refinance online but ultimately selects a home equity line instead, the sharing of sensitive personally identifiable financial information about that person for the purpose of completing the home equity line of credit application will be permitted without the imposition of any notice or consent requirements, provided the use of the sensitive information is in fact limited to the purpose of facilitating the user's loan request and application. In addition, the language "integrally related" is meant to capture any necessary sharing of personally identifiable information, however attenuated, so long as such sharing is necessary to complete the transaction, service, arrangement, or deliver the product the user requested. For example, a financial institution may provide a consolidated account statement to a customer with multiple account relationships, based on the fact that the customer has established the accounts, without the additional requirement that the customer consent before his or her personal financial information is collected and/or disclosed to an affiliated entity solely for such purposes. Finally, the "integrally related" language is meant to capture the concept of an ongoing relationship between the user and operator. For example, if a purchased product were defective, the operator that supplied the product could personally contact the user who purchased it about a product recall without violating the provisions of section 102. Or, if a product were improved (as in the case of a software upgrade, or ISP service agreement upgrade—e.g., as with AOL's periodic improvement of its ISP service from AOL 5.0 to 6.0 to 7.0 and so on), the operator that provided the product initially would be permitted to contact the user about the possibility of obtaining the product improvements without triggering the requirements of section 102.

To comply with the Fair Credit Reporting Act without regard to section 603(d)(2) of that Act, section 104(a) also certifies that the notice and consent requirements of section 102 do not apply to collection, use, or disclosure of personally identifiable information allowed under the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) so as to permit the sharing of information for credit check purposes and other similar activities authorized by that legislation. However, collection, use, or disclosure of personally identifiable information is not excepted for the purposes of compliance with section 603(d)(2) of the Fair Credit Reporting Act, which relates to commercial marketplace transactions and experiences of users, and necessarily implicates the very marketing privacy concerns ad-

dressed by the robust notice and opt-out requirements imposed in section 102.

Under section 104(b), an operator may not be held liable under the legislation, any other Federal law, or any State law, for disclosures made in good faith and following reasonable procedures in responding to requests for: (1) disclosure of personal information to the parent about his or her child as permitted by COPPA; or (2) access to, or correction or deletion of, information by users about themselves as permitted by section 105 of this legislation. Accordingly, section 104(b)(1)(A) is intended to preserve the effect of the rules adopted by the FTC pursuant to COPPA with respect to the right of parents to review and delete personal information provided by a child and the obligations of operators to permit such review and deletion, including, among other things, specifically the immunity from liability provided by 16 CFR § 312.6(b). Similarly, section 104(b)(1)(B) is intended to afford operators immunity with respect to requests for access to, or correction or deletion of, personally identifiable information under section 105 of this legislation.

In addition, a financial institution as defined under section 509(3) of the Gramm-Leach-Bliley Act may not be held liable under this legislation for any disclosure described in section 502(e) of that Act.

Under section 104(c), an operator may disclose personally identifiable information about a user to a law enforcement, investigatory, national security, or regulatory agency or department of the United States in response to a request or demand made under authority granted to that agency or department by statute, rule, or regulation, or pursuant to a warrant, court order, or properly executed administrative compulsory process. Disclosure is also permitted in response to a court order in a civil proceeding upon a showing of compelling need for the information that cannot be accommodated by any other means, provided there is reasonable notice to the user and a reasonable opportunity afforded to the user to appear and contest the order or try and narrow its scope. Any such disclosure in a civil proceeding must be accompanied by appropriate safeguards imposed by the court to protect against subsequent unauthorized disclosure of the information.

The Committee does not intend, however, that the operator shall have a responsibility to determine that the court that has issued the order has provided the appropriate safeguards referenced above. In addition, this subsection is not intended to impose upon operators an unreasonable burden of determining whether subpoenas, civil discovery devices, and other forms of process seeking the compelled disclosure of personally identifiable information operator comply with the requirements of section 4(c)(1)(B).

Under section 104(d), an operator may disclose personally identifiable information about a user or users to a law enforcement officer, hospital, clinic, or other lawful medical organization, or a licensed physician, or other health care professional if : (a) disclosure is critical to the life, safety, or health of the use or others; (b) it is not feasible to obtain timely consent in a manner consistent with the purpose of preserving life, safety, or health; and (c) the disclosure is no greater than necessary to accomplish the purpose for which the information is disclosed.

Under section 104(e), an operator may disclose personally identifiable information about a user to a provider of professional services or affiliate thereof, of which the user is a client, patient or customer, and if the provider or affiliate is subject to professional ethical standards, regulations, rules, or law requiring the provider or affiliate not to disclose confidential client information without the consent of the client.

#### *Section 105. Access*

The access provisions of section 105 are intended to provide users reasonable access to personally identifiable information without unduly burdening the party that has collected and retained that information. Operators must provide reasonable access to a user to personally identifiable information collected and retained from the user online, or that has been combined with personally identifiable information collected and retained from the user online, after the effective date of the legislation. Accordingly, operators have no obligation to retain information collected for the purpose of complying with the legislation's access requirements. If an operator collects personally identifiable information and no longer retains it, then there is no access requirement under the legislation. Moreover, the Committee wishes to clarify that the term "access" is not intended to require an operator to provide a user the ability to query directly or otherwise establish a physical or electronic connection to any database or other system of maintaining personally identifiable information. Such direct contact by the user could, while providing access, endanger security of other information collected and maintained by the operator. Rather, the term "access" contemplates that, subject to the reasonableness test set forth in this section, an operator shall provide a user a copy (electronically or otherwise) of the information the operator has collected and maintained from the user online. In addition, section 105 makes clear that "reasonable" access does not require an operator to disclose information that would compromise its ability to protect proprietary information about how it collects and stores its information.

Section 105 also requires operators to provide a reasonable opportunity for a user to suggest a correction or deletion of any personally identifiable information maintained by the operator to which the user was granted access. In addition, operators are required to make such a correction a part of the user's maintained personally identifiable information, or make the deletion requested, for the purposes of all future use or disclosure of the information.

Section 105 is not intended to create opportunities for access to personally identifiable information by impostors or persons otherwise abusing the access rights granted by the legislation. An operator may decline a suggested correction or deletion if the operator reasonably believes that the suggested correction or deletion is inaccurate or otherwise inappropriate, notifies the user of the reasons for that belief, and provides an opportunity for the user to refute those reasons. An operator need not know with certainty that a requested correction or deletion is inaccurate or inappropriate. For example, if an operator reasonably believes that the user making the request is not the actual user, the operator may deny the request. Or if the operator reasonably believes that the user's suggested correction or deletion would create an inaccuracy in the per-

sonal information maintained and collected, then the operator may deny the request.

Section 105(c) provides that reasonableness of access shall be determined by taking into account such factors as the sensitivity of the information requested to be examined, corrected, or deleted, and the burden or expense on the operator of complying with the request. However, the enumeration of such factors is not intended to exclude from consideration other factors relevant to the reasonableness of a user's request. For example, the number of requests made by a user in the past may factor into the reasonableness of a particular subsequent request. Whether the operator actually uses, or intends to use the personally identifiable information, could be a factor as well as to the sensitivity of the information requested. Or, it may be appropriate to deny access in instances to protect the safety, privacy, or other legitimate interests of third parties. Finally, the Committee does not intend this requirement to result in the reconfiguring of every operator's database so as to comply with every access request. The effort required by, and the burden and expense on, an operator in such instances should be part of the "reasonableness" analysis. The Committee must emphasize, however, that many companies on the Internet and in the offline marketplace today provide users access to their personally identifiable information. For example, Amazon.com gives users the ability to access their own personal information and edit it at their discretion. Similarly, MSN allows its users to visit the MSN Personal Information Center to view, edit or delete their personal information from the MSN database. In light of these voluntary best practices, the Committee expects the "reasonable" access requirements of the legislation to at least result in the same access by users to their personal information, once collected.

Section 105(d) provides that an operator may impose a reasonable charge for access not to exceed \$3, except in situations in which the user certifies financial hardship pursuant to the factors set forth in section 104(d)(2).

#### *Section 106. Security*

This section would require operators to establish and maintain reasonable procedures necessary to protect the security, confidentiality, and integrity of personally identifiable information maintained by the operator. This section is virtually identical to language contained in COPPA (15 U.S.C. § 6501 et seq.), which was implemented by the FTC and applies to operators (as defined therein) that collect personally identifiable information from children online. The specific FTC rule implementing this provision from COPPA required operators to "have adequate policies and procedures for protecting children's personal information from loss, misuse, unauthorized access, or disclosure." This section contemplates a similar approach and anticipates the FTC will implement its rules governing security as such.

### TITLE II—ENFORCEMENT

#### *Section 201. Enforcement by Federal Trade Commission*

Section 201 states that, except as otherwise provided, this legislation is to be enforced by the FTC.

*Section 202. Violation is Unfair or Deceptive Act or Practice*

Section 202(a) states that a violation of any provision of title I will constitute an unfair or deceptive act or practice proscribed under section 18(a)(1)(B) of the Federal Trade Commission Act. (15 U.S.C. § 57a(a)(1)(B)).

Under section 202(b), operators that are more typically regulated by other Federal and State agencies, boards, or other oversight bodies shall have their compliance with title I of this legislation enforced by those entities, under their own authorizing Acts or laws, to the same extent as if the FTC were enforcing the legislation as to those operators. Under section 202(c) for the purpose of the exercise by any agency referred to in this section of its powers under any Act or law specifically referred to in section 202(b), a violation of title I of this legislation is deemed to be a violation of a requirement imposed under that Act or law.

Under sections 202(d) and 202(e), the FTC shall enforce violations of title I in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. § 41 et seq.) were incorporated into and made a part of this legislation. This extends to penalties, privileges, and immunities provided for in the Federal Trade Commission Act. In addition, if a civil penalty is imposed on an operator in an action brought by the FTC for a violation involving non-sensitive personally identifiable information, the FTC shall hold the amount paid to the FTC in trust for distribution to aggrieved users whose information was the subject of the violation that file claims for compensation for the violation. The amount of such payment to any user shall not exceed \$200 and the FTC is required to hold monies in trust for a period of not less than 180 days. Any excess monies shall be deposited into the United States Treasury no later than 12 months after payment to the FTC.

Section 202(f) states that nothing contained in this subtitle shall be construed to limit the authority of the FTC under any other provision of law. In addition, under section 202(f)(2), nothing in title I of this legislation requires an operator to take any action inconsistent with the requirements of section 222 of the Communications Act of 1934 (47 U.S.C. 222), the provision governing the privacy of customer proprietary network information (CPNI) held by all telecommunications carriers. Finally, section 202(f)(3) amends section 631 of the Communications Act of 1934 (47 U.S.C. 51), the provision governing the privacy of cable television subscriber viewing habits and transactions, so as to apply the provisions of this legislation in place of those in section 631 when cable operators (as defined in section 631) are providing online or Internet services, or operating a commercial website (as defined in this legislation). Section 202(f)(3) would also place cable Internet services under the same privacy regime as other online and Internet services without affecting the other privacy restrictions of section 631. It harmonizes consumer Internet privacy rights without regard to whether consumers receive their Internet services over telephone lines, cable, or any other platform.

The Committee notes that the amendment made by section 202(f)(3) does not affect the continued applicability of the Electronic Communications Privacy Act, as amended by the USA PATRIOT

Act, to disclosures of personally identifiable information to law enforcement entities by cable companies in their provision of Internet services. These Acts, which were made applicable to cable operators' disclosures to law enforcement under section 211 of the USA PATRIOT Act (adding 631(c)(2)(D) to the Communications Act) remain applicable with respect to cable Internet services under section 104(c) of the bill.

*Section 203. Safe Harbor Self-Regulatory Programs*

This section incorporates one of the major changes made in the substitute amendment that was reported by the Committee. Generally, this section creates a "safe harbor" to allow self-regulatory organizations and independent third party verifiers to certify, under defined safe harbor programs, that operators are in compliance with the Act. Generally, under this section, such certification would create a presumption that the operators are in compliance with the Act. Such certifying entities are required to oversee operators' compliance with the legislation, conduct random audits of those companies, and alert the FTC of any non-compliance. In addition, any operator that is a member of a safe harbor program would be entitled to an affirmative defense in any private litigation brought by individuals aggrieved by a violation of the Act. A safe harbor will augment FTC enforcement by enabling additional oversight of companies subject to the requirements of the Act, while providing companies greater certainty that their practices and procedures are in fact compliant.

Specifically, operators shall be presumed to be in compliance with the requirements of the legislation if the operator: (1) is a participant in a self-regulatory program approved by the FTC under section 203(b); (2) has agreed in writing to meet the program's requirements for participation; and (3) is deemed by the self-regulatory program to be in full compliance with the requirements of that program.

Under section 203(b), the FTC may approve a self-regulatory program under this section only if:

(1) The program requires operators that participate in the program, at a minimum, to provide privacy protections to users that are substantially equivalent to or greater than the protection afforded to users by title I.

(2) The program reviews an operator's privacy statement and policy for compliance prior to determining its eligibility to participate in the self-regulatory program, and reviews that statement and policy no less than annually thereafter for continued compliance. As an added measure of oversight, the self-regulatory program is also required to obtain, prior to determining an operator's eligibility to participate in the self-regulatory program, and thereafter no less than annually, a written certification from a senior corporate officer or other responsible executive of the actual or prospective participant that the participant has procedures in place designed to fulfill the representations in the participant's privacy policy and satisfy, at a minimum, the requirements of the self-regulatory program. Such certification must also indicate that the participant is in compliance with the policy and the self-regulatory program's requirements.

(3) The program requires each participant to obtain written verification of each written certification required from a certified independent verification organization or provide sufficient information to the program to enable the program reasonably to conclude the certification is materially accurate. This provision creates an added check on the credibility of participants in the safe harbor and benefits compliance by requiring an independent verification of an operator's claim of compliance. In the absence of such verification, the operator seeking to participate in the self-regulatory program must provide "sufficient" (i.e. considerable and detailed) information so that the program itself can determine the operator's compliance.

(4) The program institutes a process to monitor, on an ongoing basis, the continued eligibility of program participants to ensure compliance and discover violations of the self-regulatory program's requirements. This process should include, but not be limited to, random audits of participants.

(5) The program makes available to the public on the Internet the results of audits, and violations of the program's requirements, excluding information that would reveal the identity of any complainant whose privacy was violated. Under section 203(g), however, a self-regulatory program may not be liable to any person as a result of such publication unless it is found to have acted with malice or recklessness.

(6) The program reports to the FTC as to violations of the program requirements and any determination that a participant has failed to comply with the program requirements after being afforded a reasonable opportunity to do so. This provision contemplates two reporting requirements. Any violation of the self-regulatory program guidelines would need to be reported. In addition, if a participant is informed of its non-compliance, and is given a reasonable opportunity to come into compliance but does not, the program would come under an obligation to report this type of non-compliance as well.

(7) The program establishes requirements to assure its determinations as to operators' eligibility and compliance are made exclusively by persons who are independent of the operator or participant.

Section 203(c) requires the FTC to publish a list of all violations reported to it by self-regulatory programs and independent verification organizations. In addition, the FTC is required to re-evaluate its approval of each self-regulatory program at least once every two years. The Committee intends the FTC to exercise a common sense approach in this area. If a self-regulatory program appears to be objectively and effectively handling its responsibilities, the FTC might only review its approval of that program every two years. If, on the other hand, a self-regulatory program demonstrates difficulty in complying with the requirements of this legislation, or with overseeing compliance by participants with this legislation, then the FTC may be more aggressive in its review of its approval of that program.

Under section 203(d), the FTC may certify an entity as an independent verification organization. In doing so, the FTC is required to consider both the technical expertise and experience of a prospective organization in providing assurance services. Entities eligi-

ble for such certification may be an approved self-regulatory program, provided that they are not selected to be an independent verification organization for participants that already participate in their self-regulatory program. This provision creates an added check on the credibility of participants in a safe harbor self-regulatory program and benefits compliance by requiring an independent verification of a self-regulatory program's determination that a participant is in fact complying with the program and this legislation. The FTC is also empowered by this subsection to approve any other entity as an independent verification organization provided the FTC is satisfied the entity provides assurance services and demonstrates it has the ability and knowledge to examine and evaluate the business practices of a participant or prospective participant. For example, some professional accounting firms today perform audits of operators' privacy policies. Such experience could qualify as satisfying the intent of this subsection.

Section 203(e) requires the FTC to set up an 120-day application process, including an opportunity for public comment on the application, for an entity seeking to become a self-regulatory organization. Any FTC decision can be appealed in district court.

Under section 203(f), an operator that willfully and falsely represents to the public that it is a participant in an approved self-regulatory program shall be liable for a civil penalty of up to \$50,000 for each such representation. The civil penalty imposed by this section may be recovered in an action brought by the FTC or any State attorney general.

#### *Section 204. Small Business Safe Harbor*

This section exempts from all the requirements of this legislation any entity: with annual gross revenues under \$1,000,000; with fewer than 25 employees; that collects or uses personally identifiable information from fewer than 1,000 consumers per year for purposes unrelated to a transaction with the consumer; that does not process personally identifiable information of consumers; and does not sell or disclose for consideration such information to another person. This section, offered as an amendment by Senator Brownback and adopted by voice vote in Committee, provides a common sense exemption for small businesses from the requirements of the legislation, which might prove more burdensome for them, while providing those businesses the incentive to avail themselves of the exemption by not processing, selling, or disclosing for consideration personally identifiable information. This section supplements the section 104 exceptions which exempts operators from the legislation's notice and consent requirements in those instances generally where the use of a user's personally identifiable information is solely to satisfy the request of a user. Section 204 adds to those exceptions for small businesses that only use information in such a fashion by further exempting them from the notice of policy change, notice of privacy breach, access, and security requirements of the legislation found in sections 103, 105, and 106.

#### *Section 205. Private Rights of Action by Users*

This section supplements the enforcement of the provisions of title I by the FTC and the State attorneys generals by permitting users, in those instances in which a violation occurred involving

their sensitive personally identifiable information, to pursue an action in court for both injunctive and economic relief. The approach outlined in this section tracks the approach utilized in the Telephone Consumer Protection Act of 1991, which provides for a limited right of action for consumers aggrieved by violations of that statute. It will be difficult for the FTC and State attorneys general to police all potential violations of the legislation given the thousands if not millions of operators that will be covered by the legislation. Accordingly, a majority of the Committee believes it is essential for effective enforcement to supplement those government-sponsored actions with individual rights of action, which should serve as an added deterrent to operators considering violating the statute with respect to users' sensitive personally identifiable information. The availability of a right of action for individual users will also create a process that could benefit aggrieved citizens directly, through the recovery of monetary damages.

Specifically, this section bifurcates the nature of violations and the statutory redress available to users aggrieved by violations of the legislation. First, in section 205(a), with respect to the more serious violations involving sensitive personally identifiable information—fraudulent notice or disclosure of that information—a user may bring an action in an appropriate State court where permitted by the laws or rules of a court of that State: (1) to enjoin the violation; (2) to recover actual monetary loss from the violation or receive up to \$500 for each such violation, whichever is greater; or (3) both such actions. Second, under section 205(b), if a person is aggrieved by any other violation of title I not described above (e.g., unreasonable access or unreasonable security procedures not involving disclosure), that person may have the same recourse except may not recover statutory damages of up to \$500. In such an instance, a user could bring an action, if otherwise permitted by the laws or rules of a court of a State, in an appropriate court of that State: to obtain injunctive relief or actual monetary loss with respect to the violation, or both such actions.

Subsection 205(c) provides operators an affirmative defense in any action brought under this section provided the defendant either: (1) has established and implemented with due care reasonable practices and procedures to ensure compliance with the requirements of title I; or (2) is a participant in and is deemed by a self-regulatory program or certified independent verification organization to be in compliance with a self-regulatory program under section 203.

Under section 205(d), the court is granted the discretion to increase an award to a user to not more than 3 times the amount otherwise available under this section if the court finds that the defendant willfully or knowingly violated title I.

#### *Section 206. Actions by States*

Section 206(a) permits any State attorney general to bring a civil action on behalf of residents of their State in a district court of the United States of appropriate jurisdiction with respect to any violation of title I that the State attorney general has reason to believe threatened or adversely affected an interest of residents of that State. The action may seek to: enjoin the violation; enforce compliance with the legislation; obtain damage, restitution, or other com-

pensation on behalf of residents; or obtain such other relief as the court may consider to be appropriate. This section requires an attorney general to provide prior written notice to the FTC and a copy of the complaint filed for any action brought pursuant to this section, unless the attorney general determines it is not feasible to provide the notice before filing. In such an instance, the attorney general shall provide contemporaneous notice to the FTC at the time of filing the action.

Section 206(b) grants the FTC, upon receiving a notice of an action under section 206(a), the right to intervene in the action, to be heard with respect to any matter that arises in the action, and to file a petition for appeal in the action.

Section 206(c) clarifies that nothing in this subtitle should be construed to prevent an attorney general of a State from exercising State conferred powers to conduct investigations, administer oaths or affirmations, or compel the attendance of witnesses or the production of documentary and other evidence.

Under section 206(d), in any case in which the FTC institutes an action for violation of title I, no State may during the pendency of that action institute an action under section 206(a) against any defendant named in the complaint for violation of that rule.

Under section 206(e), any action brought under section 206(a) may be brought in a United States district court that meets appropriate venue requirements, and process may be served in any district in which the defendant is an inhabitant or may be found.

#### *Section 207. Whistleblower Protection*

This section provides whistleblower protection for employees discriminated against for reporting a violation of this legislation. The Committee believes generally that many privacy violations may occur without much awareness as people's personal information may be shared without their consent, and without their knowledge. By providing whistleblower protection, the legislation would allow those in a better position to identify violations to report those violations and not suffer discrimination as a result.

Generally, this section prohibits an operator from discharging, or otherwise discriminating against, an employee because that employee provided information to any Federal or State agency or to the Attorney General of the United States or any State regarding a violation of title I. An employee or former employee who believes he has been discharged or discriminated against in violation of this section may file a civil action in the appropriate U.S. district court, and is required to file a copy of that complaint with the appropriate Federal agency. If the court determines a violation has occurred, it may order the operator to reinstate the employee, pay compensatory damages, or take other appropriate actions to remedy any past discrimination. No employee may recover under this section who deliberately caused or participated in the alleged violation or knowingly or recklessly provided substantially false information in alleging the complaint.

#### *Section 208. No Effect on Other Remedies*

The remedies provided by sections 205 and 206 are in addition to any other remedy available under any provision of law.

## TITLE III—APPLICATION TO CONGRESS AND FEDERAL AGENCIES

*Section 301. Senate*

This section requires the Senate Sergeant at Arms to develop regulations setting forth an information security and electronic privacy policy governing use of the Internet by officers and employees of the Senate that meets the requirements of title I of this legislation.

*Section 302. Application to Federal Agencies*

This section clarifies that this legislation applies to each Federal agency that is an operator to the extent provided by section 2674 of title 28, United States Code. However, this legislation does not apply to any Federal agency to the extent application would compromise law enforcement activities or the administration of any investigative, security, or safety operation conducted in accordance with Federal law.

## TITLE IV—MISCELLANEOUS

*Section 401. Definitions*

This section contains fifteen definitions necessary to implement and interpret the legislation. The legislation defines the following terms: (1) collect; (2) Commission; (3) cookie; (4) disclose; (5) Federal agency; (6) internal operations support; (7) Internet; (8) Internet service provider, online service provider, website; (9) online; (10) operator of a commercial website; (11) personally identifiable information; (12) release; (13) robust notice; (14) sensitive financial information; and (15) sensitive personally identifiable information. While it is unnecessary to restate in this report each of the definitions included in the legislation, some clarification of the Committee's intent is provided below.

(1) COLLECT.—With respect to the definition of “collect” in section 401, the Committee intends that this term will generally be interpreted consistent with the meaning of the term embodied in the FTC's implementation of COPPA. However, as further reflected in the legislation, the Committee also intends that the temporary collection or storage of information by operators of public messaging services, such as a message board, chat room, e-mail server, or instant messaging service, if temporarily collected and stored for the sole purpose of operating such public messaging service, shall not be deemed to represent a collection of personal information under this legislation.

(2) ONLINE.—With respect to the definition of “online” in section 401(9), the legislation defines “online” to refer to any activity regulated by this legislation or 18 U.S.C. 2710 that is “effected by active or passive use of an Internet connection.” The use of the term “passive” to refer to an Internet connection is intended to capture only passive methods of data collection that occur while a subscriber is actually online. Thus, the term does not include services that provide access to content cached from the Internet that do not afford a live connection between the user and the Internet, and thus no opportunity for an operator to collect personally identifiable information about the

user. For example, interactive television services that do not involve such a live connection between a user and the Internet are not subject to the requirements of this legislation.

(3) OPERATOR OF A COMMERCIAL WEBSITE.—While this term is defined as “any person with a commercial website”, it is the Committee’s intent that the FTC shall not apply the provisions of the statute to non-commercial activities of the States or Territories of the United States, or to the District of Columbia.

(4) PERSONALLY IDENTIFIABLE INFORMATION.—Section 401(11) sets forth categories of individually identifiable information about an individual such as: a first and last name; a physical address; an e-mail address; a telephone number; a birth certificate number; any other identifier the FTC finds that would create a substantial likelihood of permitting the online or physical contacting of a specific individual; or information an operator combines with any of these prior identifiers. This subsection excludes, however, “inferential information” from the definition of personally identifiable information, meaning that information an operator infers or derives about an individual from data collected online is not within this legislation’s definition of personally identifiable information. For example, if a user purchases a series of books about diabetes, or visits a health site and researches diabetes, this does not create personally identifiable information that the user has diabetes, nor personally identifiable information that the user has any specific interests in diabetes, medicine, or health. Such information would be inferential only, and only the fact that the user examined these books or websites would be personally identifiable information. Thus, if the user provided his or her name and mailing address for purchasing books and processing research about diabetes, that name and address information by itself would be deemed “personally identifiable information” but the request would not be deemed to reveal “individually identifiable health information” under section 401(15)(A). Rather, an online admission, statement, or communication that a user has diabetes would constitute such information.

(5) ROBUST NOTICE.—Section 401(13) defines “robust notice” to mean actual notice at the point of collection of the personally identifiable information describing briefly and succinctly the intent of the operator to use or disclose that information for marketing or other purposes. The Committee intends for this notice to provide a user a general level of information about the manner in which his or her personal information will be processed, if at all. Facts pertinent to such notice would include whether information will be shared with others for marketing or other purposes unrelated to the purpose for which it was provided. Such notice should also include whether the operator itself intends to use the information for marketing or other purposes unrelated to the purpose for which it was provided. One example of such notice is found at the website 1800flowers.com and is excerpted below:

“As a registered member of 1-800-FLOWERS.COM you will be receiving promotional offers and materials from us and sites and companies we own. Please check the box below if you DO NOT want to receive such materials in the future and do not

wish us to provide personal information collected from you to third parties \* \* \* In the alternative, you can utilize the procedures set forth in our Privacy Policy” (at which point a link to the complete policy is provided).

*Section 402. Effective Date of Title I*

This section states that title I of this legislation takes effect on the day after the date on which the FTC publishes a final rule under section 403.

*Section 403. FTC Rulemaking*

This section requires the FTC to initiate a rulemaking within 90 days after enactment to develop regulations to implement title I. The FTC is required to complete the rulemaking within 270 days after its initiation. The Committee believes that a rulemaking by the expert agency is required on an issue as complex as Internet privacy. Such a proceeding will afford all interested parties—industry operators, potential self-regulatory organizations, consumer groups, privacy advocates, academics, etc.—to participate and help craft governing rules to protect privacy online and provide business certainty as to what those rules will mean in practice. The Committee also notes that this mechanism was successfully utilized in implementing COPPA, which has been in effect for several years.

*Section 404. FTC Report*

This section requires the FTC to report to the Congress on outstanding issues unresolved by the legislation which may require future government action. The FTC is required to report to Congress 18 months after the effective date of title I, and annually thereafter. These reports are to focus on: (1) whether the legislation is accomplishing the purposes for which it was enacted; (2) whether pro-privacy technology is being used in the marketplace to facilitate compliance with and administration of title I; (3) whether additional legislation is needed to accomplish those purposes or improve the administration of the legislation; (4) whether and how the government could assist industry in developing standard online privacy notices that substantially comply with the notice requirements of section 102(a); and (5) whether additional legislation is necessary or appropriate to regulate the privacy of personally identifiable information collected online before the effective date of title I. This section requires the FTC to initiate a notice of inquiry, within 90 days after enactment, seeking public comment on these issues in preparation of its report.

*Section 405. Development of Automated Privacy Controls*

This section requires the National Institute of Standards and Technology to encourage and support the development of one or more computer programs, protocols, or other software, such as the P3P program, capable of being installed on computers or computer networks with Internet access that would reflect the user’s privacy preferences for protecting personally identifiable information, without requiring user intervention once activated.

## TITLE V—OFFLINE PRIVACY

*Section 501. Collection, Use and Disclosure of Personally Identifiable Information Collected Offline*

This title, added to the bill in the Hollings amendment, in the nature of a substitute, is the cosponsors' response to the concerns raised by many, primarily in the Internet industry, that it is unfair to regulate Internet privacy without requiring exactly the same rules for offline merchants and other marketplace participants that collect and trade in personally identifiable information. While this argument was not conclusive with respect to some prior statutes regulating privacy as new technologies emerged or discrete types of information warranted protection, there is some validity to the argument given the confluence of the online and offline marketplaces. However, the majority of the Committee believes that the two marketplaces are different, and the exact same approach to regulate privacy would not be feasible in each. For example, it may be more cumbersome to provide robust notice and an opportunity to opt out—exactly at the point information is collected—offline than it is online. Accordingly, this section requires the FTC to recommend, and ultimately develop, offline privacy rules similar to those required in this legislation for the Internet, but also provides the FTC the flexibility to implement rules that reflect the differences in the two marketplaces. Thus the FTC would be required to develop rules that provide notice, opt-out and opt-in opportunities (depending on the sensitivity of the personally identifiable information collected), and reasonable access and security requirements. But the FTC's offline rules would not need to mirror precisely those it promulgates for the Internet.

Specifically, section 501(a) requires the FTC to propose to Congress detailed recommendations and proposed regulations for offline privacy no later than six months after enactment. Those recommendations and regulations are to apply to entities that engage in the collection of personally identifiable information, or employ methods involving, or other actions involving, the collection of personally identifiable information, that are not covered in this legislation. Moreover, those recommendations and regulations are to seek a level of protection for personally identifiable information collected offline similar to the level of protection provided by this legislation for personally identifiable information collected online.

Section 501(b) requires the FTC recommendations and proposed regulations to address at least: how the fair information practices of notice, choice, access, security, and enforcement should apply to offline uses and disclosure of personally identifiable information; and the fines that should be established for violating requirements set forth under such proposed regulations.

Section 501(c) provides Congress at least 12 months upon receipt of the FTC proposed rules to enact a law that establishes standards for offline privacy. However, if Congress fails to act within 18 months after enactment of this legislation, then the FTC is required to promulgate final regulations within one month. Any regulation promulgated in such fashion shall supersede State law to the same extent as this legislation provides for preemption of State and local Internet privacy statutes, rules, and regulations.

## ROLLCALL VOTES IN COMMITTEE

In accordance with paragraph 7(c) of rule XXVI of the Standing Rules of the Senate, the Committee provides the following description of the record votes during its consideration of S. 2201:

Senator McCain offered an amendment, to the amendment (in the nature of a substitute) offered by Senator Hollings, to ensure that equal obligations are imposed by law on the collection, use, and disclosure of personally identifiable information online and by any other means and to suspend enforcement of the Act until such time. By rollcall vote of 9 yeas and 14 nays as follows, the amendment was defeated:

YEAS—9	NAYS—14
Mr. McCain	Mr. Hollings
Mr. Lott <sup>1</sup>	Mr. Inouye <sup>1</sup>
Mrs. Hutchison <sup>1</sup>	Mr. Rockefeller <sup>1</sup>
Ms. Snowe	Mr. Kerry <sup>1</sup>
Mr. Brownback	Mr. Breaux
Mr. Smith	Mr. Dorgan
Mr. Fitzgerald <sup>1</sup>	Mr. Wyden
Mr. Ensign <sup>1</sup>	Mr. Cleland
Mr. Allen	Mrs. Boxer
	Mr. Edwards
	Mrs. Carnahan <sup>1</sup>
	Mr. Nelson
	Mr. Stevens
	Mr. Burns

<sup>1</sup>By proxy

Senator Brownback offered an amendment, to the amendment (in the nature of a substitute) offered by Senator Hollings, to provide for reasonable network security procedures. By rollcall vote of 9 yeas and 14 nays as follows, the amendment was defeated:

YEAS—9	NAYS—14
Mr. McCain	Mr. Hollings
Mr. Lott	Mr. Inouye <sup>1</sup>
Mrs. Hutchison	Mr. Rockefeller <sup>1</sup>
Ms. Snowe	Mr. Kerry <sup>1</sup>
Mr. Brownback	Mr. Breaux <sup>1</sup>
Mr. Smith	Mr. Dorgan
Mr. Fitzgerald <sup>1</sup>	Mr. Wyden
Mr. Ensign <sup>1</sup>	Mr. Cleland
Mr. Allen	Mrs. Boxer
	Mr. Edwards <sup>1</sup>
	Mrs. Carnahan <sup>1</sup>
	Mr. Nelson
	Mr. Stevens
	Mr. Burns

<sup>1</sup>By proxy

Senator Allen offered an amendment, to the amendment (in the nature of a substitute) offered by Senator Hollings, to revise the private right-of-action provisions. By rollcall vote of 8 yeas and 15 nays as follows, the amendment was defeated:

YEAS—8  
 Mr. McCain  
 Mr. Lott  
 Mrs. Hutchison  
 Ms. Snowe  
 Mr. Brownback<sup>1</sup>  
 Mr. Fitzgerald<sup>1</sup>  
 Mr. Ensign<sup>1</sup>  
 Mr. Allen

NAYS—15  
 Mr. Hollings  
 Mr. Inouye<sup>1</sup>  
 Mr. Rockefeller<sup>1</sup>  
 Mr. Kerry<sup>1</sup>  
 Mr. Breaux<sup>1</sup>  
 Mr. Dorgan  
 Mr. Wyden  
 Mr. Cleland  
 Mrs. Boxer  
 Mr. Edwards<sup>1</sup>  
 Mrs. Carnahan<sup>1</sup>  
 Mr. Nelson  
 Mr. Stevens  
 Mr. Burns  
 Mr. Smith

<sup>1</sup>By proxy

Senator Allen offered an amendment, to the amendment (in the nature of a substitute) offered by Senator Hollings, to provide that it is not a violation of title of the Act to collect, use, or disclose personal information in compliance with other Federal laws governing privacy. By rollcall vote of 8 yeas and 14 nays as follows, the amendment was defeated:

YEAS—8  
 Mr. McCain  
 Mr. Lott  
 Mrs. Hutchison  
 Ms. Snowe  
 Mr. Brownback<sup>1</sup>  
 Mr. Smith  
 Mr. Ensign<sup>1</sup>  
 Mr. Allen

NAYS—14  
 Mr. Hollings  
 Mr. Inouye<sup>1</sup>  
 Mr. Rockefeller<sup>1</sup>  
 Mr. Kerry<sup>1</sup>  
 Mr. Breaux  
 Mr. Dorgan  
 Mr. Wyden  
 Mr. Cleland  
 Mrs. Boxer  
 Mr. Edwards<sup>1</sup>  
 Mrs. Carnahan<sup>1</sup>  
 Mr. Nelson  
 Mr. Stevens<sup>1</sup>  
 Mr. Burns

<sup>1</sup>By proxy

Senator Allen offered an amendment, to the amendment (in the nature of a substitute) offered by Senator Hollings, to broaden the pre-emption of State laws, rules, and regulations. By rollcall vote of 9 yeas and 14 nays as follows, the amendment was defeated:

YEAS—9  
 Mr. McCain  
 Mr. Lott<sup>1</sup>  
 Mrs. Hutchison  
 Ms. Snowe  
 Mr. Brownback<sup>1</sup>  
 Mr. Smith  
 Mr. Fitzgerald<sup>1</sup>  
 Mr. Ensign<sup>1</sup>  
 Mr. Allen

NAYS—14  
 Mr. Hollings  
 Mr. Inouye<sup>1</sup>  
 Mr. Rockefeller<sup>1</sup>  
 Mr. Kerry<sup>1</sup>  
 Mr. Breaux  
 Mr. Dorgan<sup>1</sup>  
 Mr. Wyden  
 Mr. Cleland  
 Mrs. Boxer

Mr. Edwards<sup>1</sup>  
Mrs. Carnahan<sup>1</sup>  
Mr. Nelson  
Mr. Stevens<sup>1</sup>  
Mr. Burns

<sup>1</sup>By proxy

By rollcall vote of 15 yeas and 8 nays as follows, the bill was ordered reported with an amendment in the nature of a substitute:

YEAS—15  
Mr. Hollings  
Mr. Inouye  
Mr. Rockefeller  
Mr. Kerry  
Mr. Breaux  
Mr. Dorgan<sup>1</sup>  
Mr. Wyden  
Mr. Cleland  
Mrs. Boxer  
Mr. Edwards<sup>1</sup>  
Mrs. Carnahan  
Mr. Nelson  
Mr. Stevens  
Mr. Burns  
Mr. Smith

NAYS—8  
Mr. McCain<sup>1</sup>  
Mr. Lott<sup>1</sup>  
Mrs. Hutchison<sup>1</sup>  
Ms. Snowe<sup>1</sup>  
Mr. Brownback<sup>1</sup>  
Mr. Fitzgerald<sup>1</sup>  
Mr. Ensign<sup>1</sup>  
Mr. Allen

<sup>1</sup>By proxy

MINORITY VIEWS OF SENATORS McCAIN, BROWNBACK,  
AND ALLEN

We strongly support the right of American consumers to protect their personal information from misuse and unauthorized disclosure by businesses and other organizations that collect such information, whether they collect and use it online or in the traditional offline marketplace. Over the past five years, the market has produced impressive advances in technology that help protect consumer privacy. These technological advances are all evidence of a burgeoning market for pro-privacy solutions in response to consumer demand. We continue to support investment and innovation in this competitive marketplace for better privacy protections, and encourage industry efforts to develop more advanced privacy tools that benefit consumers.

We also commend the Federal Trade Commission's increased efforts during this Congressional session to protect the privacy of the American consumer. Chairman Muris's newly created Privacy Task Force, the FTC's commitment of 50% more resources this fiscal year to enforcing existing Federal privacy laws, and the Commission staff's continued daily monitoring and pursuit of unfair and deceptive practices demonstrate the FTC's conviction to strictly enforce the myriad of privacy laws under its jurisdiction.

While we support the FTC's efforts to improve the protection of consumer privacy, commend advances in industry self-regulation and encourage the development of technological tools, we also believe that legislation in this area may be warranted. However, we cannot support S. 2201 as reported by the Committee. Although the cosponsors of S. 2201 may share some of our privacy goals, we fundamentally disagree with their legislative approach and oppose passage of the bill over a number of important principles.

While well-intentioned, S. 2201's approach is over-regulatory, its disparate impact on online businesses is unjustified, and its failure to reconcile its provisions with existing Federal privacy laws renders it administratively unworkable. If enacted as reported, this bill would endorse discriminatory treatment of one segment of industry by first requiring the FTC to implement privacy regulations only for those entities that have an online presence. The cosponsors amended S. 2201 during the executive session to call for "similar" regulation of offline businesses at a later date. We believe, however, that in any privacy legislation, Congress must simultaneously impose equal obligations on entities wherever their collection of personal information and potential misuse or unauthorized disclosure may occur, whether online or offline. Finally, the private right of action created in this legislation is an unnecessary enforcement mechanism that would create a greater risk of abuse to be borne by industry—particularly where S. 2201 would present conflicting obligations for companies that must comply with other Federal pri-

privacy laws—without providing any proven, increased consumer protection.

Three of the five Federal Trade Commissioners, including Chairman Muris, agree that S. 2201 is unworkable. Chairman Muris cautions that Congress needs better information about crafting effective legislation to accomplish its privacy goals, and better analyses of the costs and benefits such legislation would produce. Additionally, four of the five Commissioners question the fairness and practicality of S. 2201's limited application to online information practices, simply based on the medium used to collect information, when the collection and use of personally identifiable information is also widespread offline. The comments of each of the five FTC Commissioners on the principal features of S. 2201 were provided in separate letters dated April 24, 2002, in response to an inquiry by Senator McCain. The Commissioners' letters are reprinted (without attachments) at the end of these Minority Views.

Although the cosponsors of S. 2201 claim that the manager's amendment adopted in the executive session addressed the concerns raised by members of the Committee and the FTC, we respectfully disagree. The bill's amendments adopted at the executive session fall far short of addressing its fundamental problems. Were it to be enacted as reported, S. 2201 would impose enormous costs on American industry, and with it the national economy, without ensuring equal or greater offsetting benefits to American citizens.

#### BACKGROUND: CONSUMER PRIVACY IN 2002

This Committee Report provides a detailed history of the online privacy debate, beginning with the foundations of privacy rights in our courts and surveying the movement of the issue over the past five years. It summarizes consumer polls, e-commerce statistics, FTC surveys and reports to Congress, some dating back to 1997, as well as the legislative history beginning with the 106th Congress. This background may be important to a thorough understanding of the issue, however, the sheer breadth of this history overemphasizes the past state of privacy issues by limiting discussion of the most recent data on consumer privacy. This may leave the impression that the issues concerning consumer privacy legislation today, in 2002, are the same as they were in 1997.

Much has changed, however, in the last five years. Congress has passed new privacy legislation regulating, among other things, health, medical and children's information. The FTC has stepped up enforcement efforts and increased funding and technological capabilities to aid these efforts. Websites have overwhelmingly adopted privacy policies and improved consumer protections. Technological tools such as firewalls and anonymous browsing services have been developed and are now readily available to consumers. The widespread collection and use of personal information offline has become better known to the public and, in many ways, has remarkable similarities to online information practices. Most importantly, our national economy and way of commerce has changed dramatically, as evidenced by the growth of e-commerce and the public's widespread use of the Internet. We must understand the privacy debate and review the goals and provisions of S. 2201 with-

in today's commercial environment, and S. 2201 must be justified on grounds applicable in 2002, not 1997.

Many consumer surveys on information collection practices have been conducted over the past several years, and most Americans responding to them have indicated their concerns about the privacy of their personal information. Until recently, however, the results of these polls were often unclear about the exact nature of consumers' concerns and what they believed should be done to address them. A February 2002 survey conducted by Harris Interactive, entitled "Privacy On and Off the Internet: What Consumers Want," was designed to more closely explore consumers' attitudes regarding the handling of consumer information online and offline. The Harris poll found that consumers are most concerned about companies sharing their personal information with other companies without asking permission. However, the poll also found that more than half of those surveyed (58 percent) stated that, if they were confident that a company—whether offline or online—really followed its privacy policies, they would be likely to recommend that company to friends and family.

Increasingly, online and offline companies are responding to this growing consumer demand for better privacy protections. Although industries collecting and using consumer information online have, more often than not, opposed online privacy legislation, they argue that enforcement of existing privacy laws, coupled with self-regulatory measures, increased customer pressures and technological advancements have dramatically improved privacy protections for consumers.

In an effort to determine the necessity of online privacy legislation and the adequacy of private industry efforts to protect consumer privacy, the FTC began surveying Internet websites in 1995 to determine the extent to which they posted privacy policies informing consumers how they collected and used their information. As described in further detail in this Committee Report, the FTC completed two website surveys, in 1998 and 2000, and reported the results of these surveys and its conclusions to Congress in three annual reports during that time.

In order to provide current data comparable to the FTC's earlier studies, the Progress & Freedom Foundation (PFF) conducted a new survey in December 2001 which duplicated the previous methodology used by the FTC. The results of this extensive online survey were released in March 2002 and remain the most current data available on the status of privacy protections online. Compared to the FTC's 2000 survey, this latest survey found that the most popular websites are: collecting less personally identifiable information (decreasing from 96 percent in 2000 to 84 percent in 2001); using fewer third-party cookies to track surfing behavior across multiple websites (decreasing from 78 percent to 48 percent); providing more prominent and complete notices (nearly 100 percent of those surveyed); providing consumers with more choice over the sharing of personally identifiable information with third parties (increasing from 77 percent to 93 percent); and increasingly offering a combination of fair information practice elements, such as notice, choice, and security (sites providing all 3 rose from 63 percent to 80 percent). Most importantly, the PFF survey found that 99 per-

cent of the 85 busiest websites had posted privacy policies, and 80 percent of a random sample of websites had done so as well. Once a website has a stated privacy policy, the FTC can enforce a company's compliance with it under the FTC's traditional unfair and deceptive practices enforcement authority.

S. 2201 FAILS TO CREATE EQUAL OBLIGATIONS FOR ONLINE AND OFFLINE INFORMATION PRACTICES

The most significant problem with S. 2201 is its disparate treatment of information based on whether it is collected online or offline. Under this legislation, online providers of goods and services would be subject to more restrictive notice, consent, access, and security requirements than their offline counterparts when using similar consumer information for marketing and customer relationship management.

Information collection is not limited to the online world, and polls show that consumers are concerned about the privacy of their information regardless of where or how it is collected. Consumers are right. There is no justification for treating consumer information collected online differently from the same information collected through other means, such as through offline credit card transactions or mail-in warranty registration cards. Commenting on S. 2201, FTC Chairman Muris explained that the "sources of information that lead to our number one privacy complaint—ID theft—are frequently offline." Commissioner Swindle further noted that, "Perhaps the most glaring cost associated with the bill, and with any online-specific privacy legislation, is that it discriminates in favor of offline commerce. It is important to remember that electronic commerce currently constitutes a very small portion of all commercial activity." Imposing different obligations, and therefore different costs, on entities that do business online may very well inhibit the growth of e-commerce, thereby hurting consumers rather than helping them.

Moreover, imposing unequal standards for online and offline information would create confusion for companies that collect personal information from both online and offline sources and then merge that data together in a single consumer data file. These companies would be left with inconsistent legal obligations with respect to identical types of information and uncertainty as to which notice, consent, access, and security requirements may apply to the merged data file. Disparate obligations based on the method of collection could therefore require companies with any online presence to create and administer a two-tier privacy regime for the collection and maintenance of separately regulated data—an offline system subject to any applicable Federal or State privacy regulations (such as financial or healthcare privacy laws that typically do not discriminate on the basis of the medium over which such information is collected, used, or disclosed) and an online system subject to the conflicting privacy requirements contained in S. 2201.

Such a two-tiered system would be extremely costly and burdensome to design, implement, and manage. As Commissioner Leary noted, businesses attempting to comply with S. 2201 and other laws applying different offline standards "would be required to differentiate between online and offline information, as well as any

possible differences between the notice, choice, and security requirements in the two regulatory schemes.” Indeed, the costs would undoubtedly force some companies to discontinue their online operations altogether. The potential impact to consumers of such costs would be great. Higher costs to businesses would likely be passed on to consumers in the form of more expensive goods and services, and e-commerce in general would suffer from less competition and the loss of valuable online services if companies cease or limit their online operations. Therefore, an ironic, unintended consequence of S. 2201 is that it provides a disincentive, rather than an incentive, for companies to increase online services and consumers to use the Internet and works against Congress’s efforts to promote the growth of the Internet and e-commerce.

In light of the significantly higher administration and compliance costs associated with maintaining separate databases, some companies may consider whether maintaining any online presence at all means having one privacy compliance regime, as opposed to two. This would require these companies to subject all of their data collection practices to S. 2201’s more restrictive notice, consent, access, and security requirements (in those instances where it’s actually possible to comply with S. 2201 and the other laws’ requirements). A study released by Columbia University in January 2002, however, concluded that the increased costs imposed by a more restrictive opt-in consent requirement on financial industries alone (as would be required by S. 2201) “would take the form of higher interest rates for credit cards and mortgages, lost efficiencies in non-store retailing, lost donations to charitable organizations, and higher premiums for personal insurance policy-holders.” Such results may lead these companies to conclude there are competitive advantages to abandoning their online efforts entirely and underpricing those who continue to maintain online presences under more restrictive information collection and use practices.

In the background section of this Committee Report, the majority contends that Congress typically adopts medium-specific privacy laws when new technological media threaten consumers’ privacy. However, with the exception of the Children’s Online Privacy Protection Act of 1998 (COPPA), all other existing Federal privacy laws apply different standards based on the nature of the information collected, not on the nature of the medium. For example, the Cable Communications Policy Act of 1984 restricts some sharing of customers’ personally identifiable information, including their cable viewing habits, regardless of how it is collected. It is true that cable companies with “two-way” interactive systems could obtain viewing habit information through their cable medium, but the bill applies equally to “one-way” non-interactive cable programming providers that have no way of using the cable medium to collect viewing habits. While COPPA specifically addresses information collected over the Internet, it is a narrow exception that we are willing to tolerate to protect children online where, unlike the offline world, it is not apparent whether their parents are accompanying them.

The substitute amendment adopted by the Committee added title V to the bill, which would set in motion a process to adopt rules at a later time that would provide protection “similar to that pro-

vided under this Act” to information collected offline. Requiring only that the FTC ensure that the privacy standards for online and offline collection be “similar,” however, is insufficient to ensure nondiscrimination. Moreover, the new title establishes a separate proceeding subject to a separate schedule for separate implementation. A process that considers online and offline information separately is purely cosmetic, and destined to lead to unequal results. In order to implement privacy regulations equally online and offline, regulators must simultaneously analyze and determine which notice, consent, access, and security requirements can be effectively implemented in both settings. By separating the implementation schedules, however, S. 2201 would require the FTC to implement online regulations without knowing whether or how those same regulations could later be implemented offline, thereby ensuring disparate treatment of information collected online for at least some time, and potentially until previously adopted online regulations that will not work offline are later repealed or rewritten.

Unfortunately, attempts to resolve the inequities of S. 2201 through adoption of a manager’s amendment fell far short. Although we are not anxious to delay the enforcement of any privacy protections for American consumers, we are not willing to let unfair and unequal application of the law be the price we pay for our haste.

#### S. 2201 PERMITS PRIVATE RIGHTS OF ACTION THAT MAY RESULT IN FRIVOLOUS CLASS-ACTION LAWSUITS

As reported, S. 2201 permits private rights of action for collection, use or disclosures of sensitive personal information in violation of any provision of title I of the bill, even in the case of inadvertent disclosures where no harm has resulted. The bill would award successful plaintiffs the greater of any actual monetary harm or \$500 for each violation. This private right of action, particularly the threat of class action law suits from it, would prove enormously costly for the industries it affects—a result that would be bad for businesses and bad for consumers who, as a result, would face higher prices for goods and services from passed-on legal costs.

The potential for abuse of the private right of action is greatly enhanced by the uncertain interaction between this legislation and other Federal privacy laws. S. 2201 fails to harmonize many of its privacy provisions with a myriad of existing Federal privacy laws, particularly the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Financial Services Modernization Act of 1999 (commonly referred to as the Gramm-Leach-Bliley Act or GLBA), which cover the healthcare and financial services industries, respectively. For example, healthcare and financial services companies complying in every way with the notice, consent, access, and security requirements of HIPAA and GLBA may nonetheless be in violation of S. 2201’s differing requirements in those areas. Additionally, many provisions of S. 2201 would directly conflict with provisions in HIPAA and GLBA, leaving healthcare and financial services companies that are subject to both S. 2201 and their own industry-specific privacy law unable to legally comply with both. Legal ambiguity coupled with a private right of action is a

trial lawyer's dream. Given the conflicting obligations this bill would create for these industries, S. 2201's private right of action would virtually ensure that class-action litigation would come down on multi-billion dollar corporations that would face inconsistent laws and therefore be subject to privacy violations on the very day that rules became effective under this Act.

Proponents of private rights of action claim that they are necessary for their deterrent effect on bad actors. It is likely, however, that they do nothing to stop bad actors, but do everything to put at risk good actors who might happen to have deeper pockets. Bad actors are those that deliberately choose to violate the law, and may include disreputable companies operating outside the country or intentionally disguising their whereabouts to avoid detection. Threats of lawsuits in the United States will not deter such actors operating on a global stage that are intentionally skirting our and other nations' privacy laws.

Congress has passed many Federal privacy laws without private rights of action, including HIPAA, COPPA, and GLBA, three of the most significant privacy statutes passed in recent years. If Congress found it unnecessary to include a private right of action in legislation dealing directly with classes of highly sensitive information such as detailed healthcare and financial records, then it is unclear why a private right of action should be included in S. 2201 for broader-based regulation of health and financial information. The Committee has seen no evidence indicating that the enforcement mechanisms mandated by these privacy laws are so inadequate for ensuring compliance with their provisions that they must be supplemented with private rights of action. We should not forget that many of the most egregious examples of privacy abuses often mentioned in our debates—such as Eli Lilly and Company's inadvertent e-mail disclosure of several hundred Prozac customers' identities are already illegal acts under section 5 of the FTC Act, which makes "unfair or deceptive acts or practices in or affecting commerce," including breaches of corporate privacy policies, unlawful. As it demonstrated in its vigorous investigation of Eli Lilly, the FTC should continue to aggressively pursue privacy violations under our extensive framework of existing federal privacy laws. Unless it is shown that the FTC and State attorneys general are unable to properly enforce S. 2201, we should avoid opening the door to potential abuses such as frivolous class-action lawsuits.

Ironically, the private right of action included in this bill may encourage more consumer data collection than would otherwise occur. Companies will be forced to record and retain information on every consumer interaction to prepare themselves to defend against potentially frivolous law suits. The record for each such interaction would have to include proof that the company offered notice to the consumer, offered an opt-in or opt-out, and responded to each access request.

Another unintended consequence of S. 2201's private right of action is that it could increase the complexity of consumer notices. Some consumer advocates have argued that the notices distributed pursuant to GLBA were confusing and inadequately informed consumers of their choices regarding the sharing of their financial information. Yet, these notices were not even written with a defense

to private rights of action in mind. As Commissioner Swindle explained, some of the difficulty in complying with GLBA's notice requirements was due to the "challenge of communicating complex information to consumers," and the same challenge would also apply to S. 2201's notice and consent provisions. While it is very important that consumers have clearer and more concise notices, if companies must put their privacy policies to a jury, we can be sure that lawyers will draft them with an eye toward litigation and not intelligibility. S. 2201 may therefore exacerbate the very consumer confusion regarding notices that it seeks to remedy.

The majority of businesses covered under S. 2201's private right of action, including all financial services institutions and healthcare entities, are already subject to separate privacy regulations and separate enforcement regimes of GLBA and HIPAA. Passing S. 2201 into law would therefore create a huge and unnecessary new source of class-action litigation with no corresponding privacy benefits to consumers.

#### S. 2201 CONFLICTS WITH EXISTING FEDERAL PRIVACY LAWS

The bill leaves unanswered the complex policy question of how to superimpose a new, broad-based law for privacy practices on top of the sector-by-sector Federal privacy regime that exists today. Many industries' information practices are now separately regulated by one or more of over 20 Federal privacy laws, such as the healthcare industry under HIPAA, the financial services industry under GLBA, and the credit reporting industry under the Fair Credit Reporting Act of 1970 (FCRA). Any attempt to superimpose broad privacy regulations that would apply to only the online information practices of all industries is an extraordinarily complicated task. To be done effectively, it would require the coordination and cooperation of many Federal agencies to implement identical rules, each within its own regulatory schemes, in order to create a single Federal standard across the industries over which the agencies have jurisdiction. The bill fails to do this.

Because S. 2201 does not provide complete harmonization with the numerous Federal privacy laws that already protect the privacy of individuals, there remain very significant practical challenges to implementing S. 2201 in its current form. Care must be taken to consider the effects of this bill on existing laws, particularly if its enactment would create ambiguous or conflicting requirements for businesses and greater confusion for consumers. Unfortunately, the record in Committee illustrates the numerous ways in which S. 2201 creates inconsistent obligations for healthcare and financial services companies.

A healthcare provider or health plan subject to both HIPAA and S. 2201 would be required by S. 2201 to make available information to users under circumstances in which HIPAA does not entitle an individual to access such information, such as when the information is reasonably likely to endanger the life or safety of the individual or a third party. Additionally, S. 2201 allows a consumer to revoke consent for the use and disclosure of personal information. Yet in implementing HIPAA, regulators eliminated a similar provision after discovering that such a rule was unworkable and potentially harmful to patient care. For example, a patient's pre-

scription drug information may be needed in the future to warn that individual about a potentially fatal adverse drug reaction. Yet, patients that revoke consent over the downstream uses of their prescription drug information (as would be permitted under S. 2201) may endanger their lives by preventing healthcare providers from using the information in their records to warn them of life-threatening drug interactions.

With respect to financial information, S. 2201 applies entirely different consumer consent requirements than GLBA. S. 2201 requires affirmative prior consent, or an opt-in, for the collection, use, or disclosure of information, whereas GLBA requires an opt-out. Such a result leaves companies no choice but to knowingly violate one of the laws to which they are subject. Even where S. 2201 and GLBA appear on their face to require similar consumer notices, there are significant inconsistencies between the online notice requirements of this bill and the requirements applying both online and offline under GLBA. As a result, industry representatives contend that it's not clear that a single notice sent by a financial institution could satisfy both requirements. Financial services companies would therefore be left with choosing the lesser evil of either incurring the costs of sending two separate and differently worded notices to the same customer (an exercise likely to lead to increased consumer confusion), or risk potentially more-costly litigation for technically violating S. 2201's notice provisions despite their good faith efforts to comply with two inconsistent and conflicting laws.

#### S. 2201 FAILS TO ADEQUATELY PREEMPT STATE PRIVACY LAWS

A fundamental function of Federal privacy legislation should be preemption of multiple and inconsistent State privacy laws in order to create more regulatory certainty for businesses and correspondingly less confusion for consumers. S. 2201 fails to do this. By not preempting State common law, S. 2201 does not adequately preclude private lawsuits based on existing State common law rights of action, which may impose duties upon companies not contemplated by S. 2201 or even at odds with those mandated by the bill.

As reported, S. 2201 requires that its provisions supersede any State statutes, regulations, or rules regulating "Internet privacy." It does not mention State privacy laws that may cover businesses in both their online and offline information practices. The effect of S. 2201's preemption provisions on these other laws is therefore unclear. In particular, financial services and healthcare providers may face potentially inconsistent privacy provisions in States with financial services and medical privacy laws that do not distinguish between online and offline collection of information.

#### S. 2201 FAILS TO DEFINE REASONABLE ACCESS AND SECURITY STANDARDS

S. 2201 would create broad standards by which companies collecting personal information online must give users "reasonable access" to that information and establish "reasonable procedures necessary" to ensure the security and integrity of consumer information they maintain. While these undefined terms would require extensive FTC clarification in a rulemaking, S. 2201 fails to provide

any legislative guidance. As Chairman Muris explained, “The statute is silent, for example, on how to balance the benefits of convenient customer access to their information with the inherent risks to security that greater access would create. The FTC has no answer to this conundrum.” Indeed, the FTC had previously assembled numerous privacy experts, including industry representatives, consumer advocates and academics, to specifically examine how to implement access and security requirements in privacy legislation. This Advisory Committee on Access and Security reported to the FTC in 2000 that it could not reach consensus on how to craft workable rules to implement such provisions.

S. 2201’s extensive access requirements could cause companies that traditionally do not provide access to incur significant data system restructuring costs in order to provide that information to consumers who request it. This is particularly a concern for the financial services industry where sensitive account and transactional information is decentralized across multiple databases, some of which is constantly being processed for transactions. Likewise, others have raised security concerns particularly with respect to companies that would not otherwise create or retain consumer profiles searchable by name or other types of personal information. As noted above, S. 2201’s access obligations may even conflict with existing restrictions on access in other privacy laws, such as HIPAA. Additionally, since the private right of action would apply to violations of the access and security provisions of S. 2201, some industry representatives have suggested that a company acting in good faith may still not easily escape liability as it sought to find the right balance between access and security.

While the benefits of information security practices have never been the subject of debate, there remains a question of whether we need to legislate specific standards for them. Strong business incentives already exist for companies to provide heightened security for information they collect, particularly in their online operations. If a company’s online systems were infiltrated or “hacked,” and personal information held by them stolen, consumers would lose confidence in their business services and these companies would likely have difficulty staying in business if such lapses in security were significant or persistent. The difficulty in defining reasonable online security standards in legislation is that often the definitions of “reasonable” turn on the fact of whether a security system prevented an intrusion or not, regardless of how much effort and cost was expended by the company designing and maintaining state-of-the-art security for its website.

Recognizing the difficulties in creating security standards, S. 2201 at the very least should provide better guidance to the FTC on what is “reasonable.” A proposed solution that failed during the executive session would be to define reasonable according to the best of current industry practices on security. This approach would base reasonableness on the level of internal security mechanisms maintained by a company rather than the fact of whether a breach in a company’s online system has occurred. As the discussion in the executive session illustrated, if reasonable is merely determined on the basis of whether a breach in security could occur, this would make companies strictly liable for the slightest of security

breaches, regardless of the level of security mechanisms maintained, since any breach would be considered “unreasonable.” Such a standard would ultimately result in endless litigation every time a hacker seeks to prove that the latest in security technology has met its match.

CONCLUDING MINORITY VIEWS

Protecting the privacy of Americans is of the highest importance, but S. 2201’s approach to achieving that important goal is significantly flawed. S. 2201 will never achieve its intended purposes of improving consumer privacy protection if its major problems are left unresolved.

JOHN MCCAIN.  
SAM BROWNBACK.  
GEORGE ALLEN.

LETTERS OF FEDERAL TRADE COMMISSIONERS

FEDERAL TRADE COMMISSION,  
*Washington, DC, April 24, 2002.*

Hon. JOHN MCCAIN,  
*Committee on Commerce, Science, and Transportation,*  
*U.S. Senate, Washington, DC.*

DEAR SENATOR MCCAIN: Thank you for your letter of April 19, 2002, requesting my views on S. 2201, the Online Personal Privacy Act.

Personal privacy issues are a key priority at the Commission. Because a variety of practices can have negative consequences, consumer concerns about privacy are strong and justified. Avoiding these consequences requires a strong law enforcement presence, and we have increased by 50 percent FTC resources targeted to addressing privacy problems. Our agenda includes:

A proposed rulemaking to establish a national, do not call registry;

Greater efforts to enforce both online and offline privacy promises;

Beefed up enforcement against deceptive spam;

A new emphasis on assuming information security;

Putting a stop of pretexting;

Increased enforcement of the Children's Online Privacy Protection Act; and

New initiatives to both help victims of I.D. theft and assist criminal prosecution of this crime.

The concerns about privacy that motivate our enforcement agenda have led others, including many members of Congress, to propose new laws, such as S. 2201, the Online Personal Privacy Act. There are potential benefits from general privacy legislation. If such legislation could establish a clear set of workable rules about how personal information is used, then it might increase consumer confidence in the Internet. Moreover, federal legislation could help ensure consistent regulation of privacy practices across the 50 states. Although we should consider fully alternative methods to protect consumer privacy and to reduce the potential for misuse of consumers' information, enactment of this of general legislation is currently unwarranted.<sup>1</sup>

Five points underscore my concern about general, online privacy legislation:

1. Drafting workable legislative and regulatory standards is extraordinarily difficult.

---

<sup>1</sup>There may be areas in which new legislation is appropriate to address a specific privacy issue. This letter addresses my concerns about broad, general legislation governing online privacy issues.

The recently-enacted Gramm-Leach-Bliley Act (“GLB”), which applies only to financial institutions, required the multiple mailings of over a billion privacy notices to consumers with little current evidence of benefit.<sup>2</sup> Our experience with GLB privacy notices should give one great pause about whether we know enough to implement effectively broad-based legislation, even if it was limited to notices.

Unlike GLB, the proposed legislation deals with a wide variety of very different businesses, ranging from the websites of local retailers whose sales cross state lines to the largest Internet service providers in the world. Thus, implementation of its notice requirement will likely be even more complicated.

Moreover, the legislation adds requirements for access not found in GLB. The recommendations of the FTC’s Advisory Committee on Online Access and Security make clear that no consensus exists about how to implement this principle on a broad scale.<sup>3</sup> Perhaps reflecting these same concerns, S. 2201 grants the FTC broad rule-making authority. The only legislative guidance is the requirement that the procedures be reasonable. The statute is silent, for example, on how to balance the benefits to convenient customer access to their information with the inherent risks to security that greater access would create. The FTC has no answer to this conundrum. We do not know how to draft a workable rule to assure that consumers’ privacy is not put at risk through unauthorized access.

The inherent complexity of general privacy legislation raises many difficulties even with provisions that are conceptually attractive in the abstract. For example, the proposed legislation imposes different requirements on businesses based on whether they collect “sensitive” or “nonsensitive” personal information. Although this may be a conceptually sound approach, we have no practical experience in implementing it, and attempting to draw such distinctions appears fraught with difficulty, both in drafting regulations and assuring business compliance. Under the statute, for example, the fact that I am a Republican is considered sensitive, but a list of books I buy and websites I visit are not.

Similarly, the broad state preemption provision would provide highly desirable national uniformity. Questions about the scope of preemption would inevitably arise, however. How would the preemption provision affect, for example, state laws on the confidentiality of attorney/client communications for attorneys using websites to increase their efficiency in dealing with their clients? Moreover, what are the implications for state common law invasion of privacy torts when the invasion of privacy occurs online?

Another problem is that, except for provisions reconciling the provisions of this bill with the provisions of the Children’s Online Privacy Protection Act and certain provisions of the Federal Communications Act, there are no provisions reconciling the proposed legislation with other important Federal privacy legislation. For ex-

<sup>2</sup>I am unaware of any evidence that the passage of GLB increased consumer confidence in the privacy of their financial information. In contrast to GLB’s notice requirements, certain GLB provisions targeting specific practices have directly aided consumer privacy. For example, the law prohibits financial institutions from selling lists of account numbers for marketing purposes, and makes it illegal for third parties to use false statements (“pretexting”) to obtain customer information from financial institutions in most instances.

<sup>3</sup>The Committee’s Final Report is available at [www.ftc.gov/acoas/papers/finalreport.htm](http://www.ftc.gov/acoas/papers/finalreport.htm).

ample, it is unclear how S. 2201's requirement of notice and "opt-in" choice for disclosure of financial information collected online would be reconciled with GLB's notice and "opt-out" requirements for the same information. Nor is it clear whether a credit reporting agency's use of a website to facilitate communications with its customers would subject it to a separate set of notice, access, and security requirements, beyond those already in the Fair Credit Reporting Act.

I want to emphasize that I note these examples, not to criticize the drafting of the proposed legislation, but to illustrate the inherent complexity of what it is trying to accomplish.

2. The legislation would have a disparate impact on the online industry.

Second, I am concerned about limiting general privacy legislation to online practices. Whatever the potential of the Internet, most observers recognize that information collection today is also widespread offline. Legislation subjecting one set of competitors to different rules, simply based on the medium used to collect the information, appears discriminatory. Indeed the sources of information that lead to our number one privacy complaint—ID Theft—are frequently offline. Of course, applying the legislation offline would increase the complexity of implementation, again underscoring the difficulties inherent in general privacy legislation.

3. We have insufficient information about costs and benefits.

Third, although we know consumers value their privacy, we know little about the cost of online privacy legislation to consumers or the online industry. Again, the experience under GLB indicates that the costs of notice alone can be substantial. Under S. 2001, these costs may be increased by the greater number of businesses that must comply, by uncertainty over which set of consent procedures apply, and by the difficulty of implementing access and security provisions.

4. Rapid evolution of online industry and privacy programs is continuing.

Fourth, the online industry is continuing to evolve rapidly. Recent surveys show continued progress in providing privacy protection to consumers.<sup>4</sup> Almost all (93 percent) of the most popular websites provide consumers with notice and choice regarding sharing of information with third parties. Some of the practices of most concern to consumers, such as the use of third party cookies, have declined sharply. Moreover fewer businesses are collecting information beyond email address. These changes demonstrate and reflect the more important form of choice: the decision consumers make in the marketplace regarding which businesses they will patronize. Those choices will drive businesses to adopt the privacy practices that consumers desire.

Perhaps most important for the future of online privacy protection, 23 percent of the most popular sites have already implemented the Platform for Privacy Preferences (P3P). This technology promises to alter the landscape for privacy disclosures substantially. Microsoft has incorporated one implementation of P3P in its

<sup>4</sup>The Progress and Freedom Foundation recently released the results of its 2001 Privacy Survey, available at [www.pff.org/pr/pr032702\\_privacy\\_online.htm](http://www.pff.org/pr/pr032702_privacy_online.htm).

web browser; AT&T is testing another, broader implementation of this technology. By the time the Act's disclosure regulations might reasonably take effect,<sup>5</sup> the technological possibilities for widespread disclosure may differ substantially. Although S. 2201 anticipates this development by requiring the National Institute of Standards to promote the development of P3P technology, legislation enacted now cannot take advantage of such nascent technology. Moreover, it may inadvertently reduce the incentives for businesses and consumers to adopt this technology if disclosures are required using other approaches.

5. Diversion of resources from ongoing law enforcement and compliance activities.

Finally, there is a great deal the FTC and others can do under existing laws to protect consumers privacy. Indeed, since 1996, five new laws have had a substantial impact on privacy-related issues.<sup>6</sup> We should gain experience in implementing and enforcing these new laws before passing general legislation. Implementation of yet another new law will require both industry and government to focus their efforts on a myriad of new implementation and compliance issues, thus displacing resources that might otherwise improve existing privacy protection programs and enforce existing laws. Simply shifting more resources to privacy related matters will not, at least in the short term, correct this problem. The newly-assigned staff would need to develop the background necessary to deal with these often complex issues. The same is likely true for business compliance with a new law. Without more experience, we should opt for the certain benefits of implementing our aggressive agenda to protect consumer privacy, rather than the very significant effort of implementing new general legislation.

Conclusion.—We share the desire to provide American consumers better privacy protection and to ensure that American businesses face consistent state and Federal standards when handling consumer information. Nonetheless, we believe that enactment of this general online privacy legislation is premature at this time. We can better protect privacy by continuing aggressive enforcement of our current laws.

Sincerely,

TIMOTHY J. MURIS,  
*Chairman.*

---

FEDERAL TRADE COMMISSION,  
*Washington, DC, April 24, 2002.*

<sup>5</sup>Again, GLB is instructive. It was almost two years between the enactment of the statute and the effective date of the privacy rules promulgated thereunder.

<sup>6</sup>Fair Credit Reporting Act, 15 U.S.C. § 1681 (amended 9/30/96); Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320 (enacted 8/21/98); Children's Online Privacy Protection Act, 15 U.S.C. § 6501 (enacted 10/21/98); ID Theft Assumption & Deterrence Act, 18 U.S.C. § 1028 (enacted 10/30/98); GLB, 15 U.S.C. § 6801 (enacted 11/12/99). Moreover, since 1996, the FTC has been applying its own statute to protect privacy.

Re S. 2201 (The Online Personal Privacy Act).

Hon. JOHN MCCAIN,  
*Ranking Member, Committee on Commerce, Science, and Transportation, U.S. Senate, Washington, DC.*

DEAR SENATOR MCCAIN: I am pleased to provide my views on S. 2201, the Online Personal Privacy Act, which was introduced by Chairman Hollings on April 18, 2002. Although I share the view of the sponsors of this legislation that privacy is important to American consumers, there has been no market failure that would justify the passage of legislation regulating privacy practices concerning most types of information. Even if such a market failure exists, I am not persuaded that the benefits of such legislation, including the proposed Online Personal Privacy Act, exceed its costs.

Indeed, the best means of protecting consumer privacy without unduly burdening the New Economy is through a combination of industry self-regulation and aggressive enforcement of existing laws that are relevant to privacy by the FTC and other appropriate regulatory agencies. This approach is flexible enough to respond rapidly to technological change and to the tremendous insight we are gaining from the ongoing dialogue among government, industry, and consumers on privacy issues.

You have asked for my assessment of whether legislation is needed. I believe legislation should be reserved for problems that the market cannot fix on its own. To my knowledge, there is no evidence of a market failure with respect to online privacy practices, nor are there signs of impending market failure that would warrant burdensome legislation. As a result of a continuing and energetic dialogue among industry, government and consumer representatives, industry is stepping up to the plate and leading the way toward enhancing consumer privacy online. Flexible and efficient privacy tools are increasingly addressing consumer concerns. Indeed, the evidence indicates that the market is responding to consumers' concerns and demands about privacy.

A recent Progress and Freedom Foundation study<sup>1</sup> tells us that there has been a significant decline in the amount of personal information that websites are collecting from visitors.<sup>2</sup> At the same time, there has been an increase in the voluntary adoption of privacy practices. The study indicates that privacy policies have become more common and more consumer-friendly over the past year. In addition, the percentage of the most popular sites offering consumers a choice whether their information can be shared with third parties increased from 77% in 2000 to 93% in 2001. The privacy-enabling technology, Platform for Privacy Preferences (P3P), is being deployed rapidly, and industry has generally become more responsive to the privacy concerns of consumers.

These trends clearly demonstrate that the online marketplace is dynamic, and that firms are working hard to find the "right" pat-

<sup>1</sup>Adkinson, William F. Jr., Jeffrey A Eisenach, Thomas M. Lenard, Privacy Online: A Report on the Information Practices and Policies of Commercial Web Sites. Washington, D.C.: Progress & Freedom Foundation (2002). Available at: <<http://www.pff.org/publications/privacyonlinefinalael.pdf>>.

<sup>2</sup>Among the most popular 100 sites, the proportion collecting personal information fell from 96% in 2000 to 84% in 2001. Similar to this finding, the proportion of those firms employing "cookies" fell from 78% to 48% in the past year.

tern for information management practices. In addition, the survey results show that the most frequently visited websites (and much of the Internet as a whole) have clearly recognized that information management policies and privacy practices are necessary parts of everyday business on the Internet. Consumers expect privacy protection and firms realize that it is to their competitive advantage to respond to customer expectations. To the extent that consumers have demanded privacy, these results show that the market had provided it.

Contrary to arguments by proponents of legislation that consumers' privacy concerns are retarding the growth of electronic commerce, electronic commerce is growing rapidly without new privacy legislation. Online transaction have roughly doubled each year between 1997 and 1999, and annual consumer purchases have risen from roughly \$5 billion in 1998 to \$32 billion in 2001. Recent data on online holiday shopping are even more dramatic, rising from roughly \$1 billion in 1997 to nearly \$14 billion in 2001—a 1300% increase. E-commerce thus is growing rapidly in the absence of new privacy regulation.<sup>3</sup>

For many years now, it has been my understanding that Congress seeks to weigh the costs and benefits of new legislation, with the goal of avoiding doing more harm than good. To my knowledge, there is no evidence concerning the costs associated with the proposed legislation, nor an assessment of whether those costs are outweighed by the ill-defined economic benefits that might follow. I do not believe legislation should be adopted without careful consideration of the problem it may create.

Perhaps the most glaring cost associated with the bill, and with any online-specific privacy legislation, is that it discriminates in favor of offline commerce. It is important to remember that electronic commerce currently constitutes a very small portion of all commercial activity. It is difficult to understand drawing a distinction between offline and online privacy. I would suggest that it is likely that consumers share similar concerns in both situations. I believe it is essential to consider the costs and benefits of regulating both online and offline privacy before any legislation is enacted.

To evaluate other costs associated with the notice and choice requirements of the Online Personal Privacy Act, the Commission's experience with the Gramm-Leach-Bliley Act (GLB Act) is instructive. The GLB Act requires that financial institutions issue privacy notices to their customers and, in certain circumstances, provide them with the opportunity to opt out of disclosures of nonpublic personal information to nonaffiliated third parties. To comply with the GLB Act last year, firms incurred great expense in disseminating privacy notices, yet very few consumers opted out. Among the difficulties encountered in complying with GLB Act was the challenge of communicating complex information to consumers. Industry would face these same challenges in communicating notice

---

<sup>3</sup>It is interesting to compare the growth of electronic commerce to the growth in the use of debit cards. Between 1988 and 1996, debit transactions slowly rose from virtually nothing to less than \$50 billion annually. As consumers' experience with these cards increased, however, debit card spending jumped to \$300 billion in 2000. This massive growth in debit card transactions was not caused by federal regulatory action, but resulted from consumers' positive experiences with the cards.

and choice in the online context, and a requirement to provide “robust” notice to consumers does little to solve these problems. It also would be difficult for static regulation to keep pace with technology. For example, regulation mandating notice provided on a website may be inapplicable to Web-enabled handheld devices, such as cell phones.

A requirement to provide “reasonable access and security” is difficult to define. In its May 2000 report, the Commission’s Advisory Committee on Online Access and Security was unable to reach consensus as to the amount and type of access that should be provided to consumers.<sup>4</sup> Given the complexity of this issue, I do not believe that it is a suitable topic for broad-based legislation or regulation. More important, the Commission already has the ability to address security breaches through the enforcement of existing statutes.<sup>5</sup>

In addition, I am not aware of reliable information about the likely costs associated with providing access and, in particular, the costs of maintaining a clickstream database that could be easily accessible to consumers and easily altered.<sup>6</sup> I therefore question whether the \$3.00 fee allowed by S. 2201 for consumers to obtain access to their information would be sufficient to cover the expense. Although some firms—obviously the larger ones—might be able to absorb the costs associated with this access mandate, other firms might be unable to provide the service for a minimal fee and would be unable to continue business with their current model. This possibility seems terribly unfair to small business and harmful to competition in electronic commerce.

Finally, in an attempt to empower consumers, this legislation gives them a private right of action. While this measure is aimed at increasing compliance with the law, I fear that a private right of action may result in unintended consequences. More specifically, increased private litigation over information management policies may chill further innovation on the part of businesses that may fear that any change in their information management practices will be met with lawsuits.

In summary, the electronic marketplace is still evolving. Industry and government have been working diligently to address consumers’ privacy concerns. Businesses have made admirable progress over the past several years and have no intention of standing down. Industry leaders are directly involved in seeking solutions to meet consumer demands and concerns. From a business standpoint, it just makes good sense. Now is not the time for the federal government to legislate and effectively halt progress on these self-regulatory efforts. New, complicated, and ambiguous laws will force innovation and investment to take a back seat to compliance and bureaucratic process. At the end of the day, we will

---

<sup>4</sup>In 1999, the Commission established an Advisory Committee on Online Access and Security to provide advice and recommendations to the Commission regarding implementation of reasonable access and adequate security by domestic commercial websites. The Committee’s final report to the Commission on May 15, 2000, described options for implementing reasonable access to, and adequate security for, personal information collected online and the advantages and disadvantages of each option.

<sup>5</sup>See *In the Matter of Eli Lilly and Co.*, FTC File No. 012 3214 (consent agreement accepted, Jan. 17, 2002) (alleging that Eli Lilly unintentionally disclosed personal information collected from consumers by not taking appropriate steps to protect the confidentiality and security of that information).

<sup>6</sup>Under the proposed legislation, clickstream data, as collected by third-party cookies, are considered to be personally identifiable information to which consumers should have access.

have made far less progress in finding solutions to privacy concerns than we would have if we had simply relied on government and private sector cooperation and market forces.

Thank you for the opportunity to offer my views on these issues. I look forward to working with you in the future.

Sincerely,

ORSON SWINDLE,  
*Commissioner.*

---

FEDERAL TRADE COMMISSION,  
*Washington, DC, April 24, 2002.*

Hon. JOHN MCCAIN,  
*Committee on Commerce, Science, and Transportation,*  
*U.S. Senate, Washington, DC.*

DEAR SENATOR MCCAIN: You have asked that members of the Federal Trade Commission provide their individual views on a privacy bill, "The Online Personal Privacy Act," S. 2201, and I am pleased to respond.

It is important to express one important reservation up front. This statement of my individual views is constrained by my understanding of the context of your request. Like any other citizen, I have personal views on fundamental issues in the privacy debate (e.g., the question of whether it is appropriate to speak of a "right to privacy" in the context of private consensual transactions as opposed to intrusions by government; the balance between any privacy rights of one party and the First Amendment rights of another; and the question of whether it is realistic to expect that most barriers to disclosure will prove effective in the long term). However, there is no reason why you or any other lawmaker should be particularly interested in my opinions about these value-laden issues, so I understand that you are asking for my views in the context of the responsibilities and capabilities of the Federal Trade Commission. In other words, this response is constrained by an appreciation of the limitations of our institutional expertise.<sup>1</sup>

To be blunt, I do not believe it is my place to advise Congress on the bottom line issue of whether it is or is not a good idea to legislate on privacy issues. (To the extent I presumed to do so in the past, I have changed my mind.) The Federal Trade Commission, in my view, functions best as a facilitator, which attempts through law enforcement and education<sup>2</sup> to ensure that consumers are not misinformed about the goods and services that they buy and that sellers are not disabled by illegal private constraints. But, in the absence of Congressional direction to the contrary, we are neutral about the terms of sale that are freely determined. We have strong institutional confidence in the ability of adequately informed consumers to make their own choices about what they want (including, presumably, varying levels of privacy protection) without interference from government. We are good at specifying what

<sup>1</sup>My previous statement on privacy issues are enclosed with this letter.

<sup>2</sup>The Commission also provides a forum for the exchange of views among outside individuals and groups.

is adequate disclosure of the terms of sale but we are not good at devising rules for what the terms of sale should be.

With this awareness of our limitations, I join with those colleagues who express serious reservations about the “Online Personal Privacy Act,” S. 2201. I generally concur in their conclusions, but write separately to emphasize my particular perspective. I simply do not believe that S. 2201 can be enforced in a coherent way. The following is a summary list of the reasons:

1. I do not believe it is workable or reasonable to treat privacy differently in the online world than in the offline world to the extent that the information collected is the same, regardless of the site of collection or the means of dissemination. It is obvious that different modes of disclosure might be required, but it is illogical to regulate one medium and not the other.

2. Congress may, in its judgment, determine that it is appropriate to mandate some form of “notice” to consumers about what will happen to their personal information. For one thing, mandated notice would eliminate the present awkward situation whereby a company that volunteers information about its privacy policy<sup>3</sup> risks prosecution if the information is inaccurate, but one that volunteers nothing risks nothing.<sup>4</sup> Recent experience with mandated notice, however, suggests that it is not enough for Congress simply to require that it be done.<sup>5</sup> Businesses have to be given more precise guidance about the forms of notice that will be useful to consumers. This is something the Federal Trade Commission, as an institution, knows something about. It might be appropriate to direct the Commission or some other appropriate body to survey the quality of notices that are either voluntarily provided or mandated today, and then recommend a template for notice that would be meaningful. This project would inform the policy debate and ultimately, perhaps, provide the framework for legislation.

3. The issue of “choice” or “consent” is much more complex than the bill seems to recognize. At first glance, it seems obvious that the whole purpose of notice is to enable consumers to make informed choices. It is necessary, however, to think about the consequences of choice. If there is no cost or reduced benefit associated with the choice to opt-out (or failure to opt-in) then the added expense of accommodating these choices will be borne by consumers less tender of their privacy. (No one suggests that people who do not want to use their supermarket charge cards because of the information disclosed should be entitled to the discount anyway.) On the other hand, if privacy-conscious consumers are disadvantaged too much, their only practical “choice” is to seek another provider, and mandated “opt-outs” or “opt-ins” become essentially meaningless. There would have to be some regulatory regime to determine what is a reasonable in-between position in these circumstances, and I have no idea how this could be done across-the-board.

<sup>3</sup>And, apparently, an overwhelming majority do, according to the most recent evidence. William F. Adkinson, Jr., Jeffrey A. Eisenach and Thomas Lenard, Progress & Freedom Foundation, “Privacy Online: A Report on the Information Practices and Policies of Commercial Websites” <[www.pff.org/pr/pr032702privacyonline.htm](http://www.pff.org/pr/pr032702privacyonline.htm)>.

<sup>4</sup>The vendor may, of course, incur marketplace risk.

<sup>5</sup>Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6810; and Interagency Public Workshop: Get Noticed: Effective Financial Privacy Notices (December 4, 2001) <<http://www.ftc.gov/bcp/workshops/glb/index.html>>.

4. Under the bill, further refinements of “access” and “security” would presumably need to be spelled out in rulemaking proceedings.<sup>6</sup> As I have said before, “[i]t is not appropriate to defer all the tough issues for future rule-making.”<sup>7</sup> I personally believe, for example, that there is a vast disparity between the costs and the minuscule benefits of an access regime in most situations, and I further believe that the costs of merely developing and enforcing across-the-board rules would also vastly exceed the benefits. Congress may want to consider whether any tailored expansions of present rights is necessary,<sup>8</sup> but a blanket mandate of “access” right is unlikely to result in significant benefits overall.

These are major objections, but the following issues are also significant:

5. S. 2201 distinguishes “sensitive” from “non-sensitive” personal information.<sup>9</sup> These categories seem arbitrary. For example, as Chairman Muris points out in his letter to you of this date, some might feel that information about the books they read is a lot more sensitive than their political affiliation. Moreover, information that is merely, “inferred” from data<sup>10</sup> may be just as sensitive as information “about”<sup>11</sup> certain aspects of an individual.<sup>12</sup>

6. The distinction between “clear and conspicuous” notice and “robust” notice<sup>13</sup> seems unworkable as a legal mandate. Articulation of the latter undercuts the significance of the former. If some form of notice is ever mandated by Congress, it should be both.

7. The bill is silent about the extent to which privacy protections travel with consumers’ personal information. In general, Gramm-Leach-Bliley’s privacy provisions require downstream recipients of covered data only to use the information in a fashion that is consistent with the consumers’ stated privacy preferences or only for uses that are exempted from the notice and choice requirements (such as credit reporting). In this sense, the protections flow with the information. I seriously question whether this concept can be applied across the economy, but without it, the privacy protections of the bill may be nullified.

8. As Chairman Muris notes, some of the provisions of S. 2201 attempt to reconcile the legislation’s privacy protections with other federal statutes that allow limited but beneficial information sharing. However, as currently drafted, S. 2201 might limit a variety of legitimate and beneficial information sharing which covered entities engage in and which Congress would like to continue. It is not clear, for example, whether information about transactions completed online could be communicated to credit bureaus. Without ap-

<sup>6</sup>S. 2201, Section 403

<sup>7</sup>Federal Trade Commission, “Online Profiling: a Report to Congress” (Part 2) (Statement of Commissioner Thomas B. Leary, Concurring in Part and Dissenting in Part) (July 2000), <<http://www.ftc.gov/os/2000/07/onlineprofiling.htm#LEARY>>.

<sup>8</sup>The Fair Credit Reporting Act, 15 U.S.C. 1681 et seq., and the Children’s Online Privacy Protection Act of 1998, 15 U.S.C. 6501 et seq. are among the federal laws that grant access rights.

<sup>9</sup>S. 2201, Sections 102 and 401.

<sup>10</sup>S. 2201, Section 401.

<sup>11</sup>S. 2201, Section 401.

<sup>12</sup>See, In the Matter of Eli Lilly and Co., FTC File No. 012–3214 (January 18, 2002), <<http://www.ftc.gov/opa/2002/01/elililly.htm>>. This case involved the improper disclosure of the identify of people who had regularly obtained information about a certain psychotropic medication, but did not disclose whether they actually took the medication.

<sup>13</sup>S. 2201, Sections 102 and 401.

appropriate exclusions, any proposed privacy rules could have a serious anti-consumer impact.

9. This bill would add to the emerging patchwork of federal privacy regulations that apply to personal information<sup>14</sup> and may ultimately result in ambiguous, conflicting, or impractical requirements for businesses, and greater confusion for consumers as well. For example, S. 2201 provides that “sensitive” and “non-sensitive” information would be subjected to different levels of protection. Dissemination of “sensitive” information would be subject to consumer notice, opt-in choice, access and security. “Non-sensitive” information would be protected by “robust” notice, opt-out choice, access and security. The specifics of these requirements would all be defined in a future rulemaking. At the same time, “non-public” personal information collected by financial institutions (whether online or offline) would be subjected to Gramm-Leach-Bliley’s distinct notice, choice and security standards.

Businesses that seek to comply with both of these regulations would be required to differentiate between online and offline information as well as any possible differences between the notice, choice, and security requirements in the two regulatory schemes. Additionally, our experience to date with Gramm-Leach-Bliley suggests that consumers may need less rather than more complex privacy disclosures in order to understand and execute their rights. It is unrealistic, at this point, to assume that consumers will comprehend the various categories of information as well as the protections that are attached to each category of information.

10. The bill provides that “penalties” would be imposed for a violation of the statute, and that “redress” would be distributed to consumers in an amount not to exceed \$200 (for breaches involving non-sensitive personal information). This confuses two separate concepts. Penalties are calculated without regard to consumer injury or ill-gotten gains, and are paid to the Treasury. Redress is intended to make consumers whole.

11. Wholly apart from the burden issues identified above, the bill does not seem to recognize the potential conflict between access and security. Broad access rights will lead to the centralization of data which could result in very significant security breaches. This is a highly technical subject, where there is no consensus among experts.<sup>15</sup>

<sup>14</sup> Among the many federal privacy laws are: Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6810 (covers financial institutions, non-public personally identifiable information and requires notice of information practices and an opt-out for sharing information with third parties); Children’s Online Privacy Protection Act, 15 U.S.C. § 6501 (covers Web site operators, prohibits collection, use and disclosure of children’s online information without verifiable parental consent and provide for parental access rights and imposes security requirements); Fair Credit Reporting Act, 15 U.S.C. § 1681 (1970) (covers credit bureaus and providers and users of credit data and grants consumers with access rights and opt-out rights for certain uses of credit data); and Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 262(a), 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29 and 42 U.S.C.A.); 42 U.S.C.A. 1320d–8 (West Supp. 1998) (covers a variety of health-related entities and health information and requirements that include notice, varying degrees of choice, access, and security).

<sup>15</sup> Final Report of Federal Trade Commission Advisory Committee on Online Access and Security, published as Appendix D of Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress (May 2000).

I appreciate the opportunity to provide these comments and would be pleased to respond to any further questions.

Sincerely,

THOMAS B. LEARY.

---

FEDERAL TRADE COMMISSION,  
Washington, DC, April 24, 2002.

Hon. JOHN MCCAIN,  
*Committee on Commerce, Science, and Transportation,*  
*U.S. Senate, Washington, DC.*

DEAR SENATOR MCCAIN: In anticipation of the Senate Commerce Committee's April 25, 2002 hearing on S. 2201, the Online Personal Privacy Act ("OPPA"), you have asked each Commissioner of the Federal Trade Commission to comment on whether legislation is needed and, if so, what such legislation should contain. As you know, the FTC has long been involved with the issue of consumer privacy and I have also personally devoted a great deal of time and thought to this matter. Accordingly, I appreciate the opportunity to offer my views about privacy legislation and comment on the principal features of the OPPA.

In the past, a particular area of focus for me has been the question of whether federal legislation is necessary. In the Commission's May 2000 Congressional Report, "Privacy Online: Fair Information Practices in the Electronic Marketplace," a majority of the FTC recommended that Congress enact online privacy legislation. In my accompanying statement and written testimony, I expressed my support for thoughtful and balanced online privacy legislation that is coupled with meaningful self-regulation and enforcement of existing laws.<sup>1</sup> I also stated that such privacy legislation should incorporate the well-established fair information practice principles of notice, choice, access and security and should provide for federal preemption of inconsistent state laws. Further, legislation should be organic and sufficiently flexible to take into account the type and sensitivity of the data at issue.

My conclusion has not changed and, as discussed below, I believe that today's market conditions make an even more compelling case for legislation. Moreover, I support the OPPA because it contains the above described elements and represents a thoughtful, balanced and well-reasoned approach to the privacy issue.

*On-line Privacy Legislation Is Needed*

Consumer confidence is one of the most important features of American economic strength and, as demonstrated by recent declines in dot-com industries, emerging markets and young industries are particularly vulnerable to consumers uncertainty. It is not surprising then, that those industries involved in the developing electronic marketplace, or "e-commerce," have begun to direct greater attention and more resources to strategies that address

---

<sup>1</sup>This position represented a change from my prior opinion which did not support legislation but, instead, called for industry self-regulatory measures. Compare Statement of Commissioner Mozelle W. Thompson Before Senate Comm. On Commerce, Science and Transp. (May 25, 2000), with Statement of Commissioner Mozelle W. Thompson Before Senate Comm. On Commerce, Science and Transp. (July 13, 1999).

consumer confidence. Members of this industry are asking what is needed to allow e-commerce to reach its potential and fully develop into a stable and robust market? One answer is data privacy.

Studies continue to indicate that consumers' foremost concern with respect to e-commerce is the privacy of their personal data. Indeed, last year Forrester Research estimated that consumers' online privacy concerns cost \$15 billion of potential e-commerce revenue. Also, 73% of online consumers who refused to purchase online did so because of privacy concerns. Moreover, one need only compare the stock prices of those companies engaged in online profiling, before and after settling complaints about their business practices, to find a clear example of the value to consumers of certainty and confidence in a new market.

To date, the FTC has provided a strong privacy foundation by way of the agency's law enforcement regime combined with our efforts in promoting industry self-regulation. Although consumers and businesses involved in e-commerce have benefitted from these efforts, they are no longer sufficient because there are still online companies that fail to protect consumer information. Without a legislative backdrop, too much of the risk of e-commerce is shifted to the consumer at a time when consumer confidence is critical. Law enforcement measures are by their nature retroactive, focusing on events that have already occurred. Once a consumer has lost his or her privacy—be it through identity theft, the creating of an unauthorized profile based upon the consumer's online activities or by some other means—it is generally impossible to make that consumer whole again.

This condition is made more serious because the Internet allows instantaneous, inexperience and unlimited transmission of data while computer databases permit storage and unprecedented manipulation. Moreover, it is difficult for the consumer to even know that his or her privacy has been violated until, in some cases, years after the fact.<sup>2</sup> Consequently, without legislation, e-commerce will remain an uncertain marketplace in which only those consumers on the fringe will participate.

The absence of legislation also forces the Commission into the unusual position of going after the good actors that have strong privacy policies, while the bad remain largely unreachable by agencies like the FTC, thus leaving these businesses free to violate consumer trust. Without the type of legislation backdrop that the Commission called for in 2000, and which OPPA provides. I am afraid there will continue to be many free riders and companies with inadequate information practices.

#### *Necessary Elements for Effective Privacy Legislation*

I believe that the OPPA addresses many of the most delicate problems associated with a legislative privacy framework. First, it contains the fair information principles and allows for flexibility and change. The OPPA avoids a "one size fits all" approach to the notice requirements and provides a reasonableness test for access. The OPPA is also more reflective of a "real world" consumer envi-

<sup>2</sup>These features, coupled with technology that allows websites to surreptitiously collect consumer information, distinguish the on-line consumer environment from the off-line world.

ronment because it employs a sliding scale that affords more protection to more sensitive information.

Second, by preempting state law, the OPPA will prevent the possibility of multiple standards that could “Balkanize” e-commerce and prove overly burdensome to business and too confusing for consumers. Finally, in granting the FTC rulemaking authority, the OPPA will permit strong enforcement, with special sensitivity to industry and consumer needs, while also providing a means for state participation.

Thank you again for providing me with this opportunity to discuss privacy legislation and the OPPA. I also hope that you will continue to consider the FTC a resource as your work progresses on this important issue.

Sincerely yours,

MOZELLE W. THOMPSON.

---

FEDERAL TRADE COMMISSION,  
*Washington, DC, April 24, 2002.*

Hon. JOHN MCCAIN,  
*U.S. Senate, SROB,  
Washington, DC.*

DEAR SENATOR MCCAIN: Thank you for your letter of April 19, 2002 asking me to comment on Chairman Hollings Senate Bill 2201, “The Online Personal Privacy Act.” Your letter asked two questions: First, whether I believe legislation is needed, and if so, what it should contain. Second, you asked for my comments on the principal features of S. 2201.

#### I. IS LEGISLATION NEEDED?

Yes, legislation is needed to protect consumers’ privacy. Absent federal standards to be followed by all persons and entities that collect private information, it is unlikely that consumers will be adequately protected from identity theft, commercial harassment, and hucksterism. In addition, dissatisfaction with and mistrust of online business practices by the American people will continue to grow; an uneven patchwork of state laws will proliferate; and consumer confidence in e-commerce will be undermined.

Industry has not been able or willing to effectively self-regulate. While some responsible companies have stepped up to the plate, the financial incentives work against a universal commitment by e-business to provide effective privacy protection for consumers. Business interests will undoubtedly point to a recent Progress and Freedom Foundation survey as evidence that federal legislation is not necessary because websites are collecting less personally identifiable information and privacy notices are prevalent, more prominent, and more complete. These arguments completely miss the mark. First, the survey reveals that nearly all sites surveyed continue to collect personally identifiable information.<sup>1</sup> Second, the

---

<sup>1</sup>The survey indicated that 90 percent of the random sample, and 96 percent of the most popular sites, collect personally identifiable information compared with 97 percent and 99 percent in 2000. This is hardly a statistically significant decline. In fact, an April 11, 2002, New York Times article (attached) chronicled how some of the Internet’s most frequently visited sites are expanding their collection and commercial use of personally identifiable information.

mere posting of a privacy policy does not ensure effective consumer protection and often is only pretty packaging of empty content.

Just any legislation is not enough. In my view, strong privacy legislation should:

- preempt inconsistent or weaker state law;
- incorporate effective notice and choice, adequate access, reasonable security, and strong enforcement remedies;
- be free from exceptions created for special interests or industries;
- require affirmative consumer consent before sensitive personally identifiable information is collected through any means either online or offline; and
- avoid tactics that unduly delay the effective date of the Act.

## II. SENATE BILL 2201

Senate Bill 2201 provides long-awaited, strong protection measures for consumers in the online world. My only concern with this proposed legislation is its limited reach. In my view, federal legislation is necessary to protect the privacy of personally identifiable consumer information in the offline as well as online commercial realms. These marketplaces are often intertwined and indistinguishable. In fact, I believe that the wired world facilitates the effective, constant aggregation of endless variety of real-time “surfer” information and combines it with commercial information gathered through traditional “offline” means. I would strongly support the expansions of this Bill’s consumer protections—to the “offline” collection of personally identifiable consumer information.

That said, Senate Bill 2201 is a balanced, comprehensive approach to protecting consumer privacy online. By incorporating the concepts of notice, choice, access, security, and enforcement, it creates a level playing field for both consumers and industry. However, I offer the following comments

### *Preemption*

I believe that federal legislation should preempt inconsistent and weaker state privacy laws which do not effectively protect consumers and tend to frustrate the development of e-commerce. On the other hand, I generally support the power of states to enact legislation that offers their citizens stronger consumer protections than federal law where the federal law merely establishes a “floor” of minimum protection standards. However, if passage of a federal law “with teeth,” is feasible. I believe that both consumers and industry would value the uniformity and predictability that federal preemption offers.

### *Title I—Online Privacy Protection*

#### *Section 101*

I applaud Title I’s coverage of personally identifiable information that is collected, used or disclosed. Previous bills focused only on the “collection” of information, yet many privacy breaches occur when information is used or disclosed without the consumer’s knowledge or consent after collection.

### *Notice and Consent*

I strongly support the inclusion of Section 102(b) which requires a consumer's affirmative consent ("opt-in") before, or at the time that, certain sensitive information is collected. An opt-in consent requirement guarantees consumer notice and meaningful choice, and compels the collector to clarify its practices in order to entice the consumer to agree to them. It effectively equalizes the bargaining position of consumers and e-merchants in the market for personal information.

While I prefer an opt-in standard for the collection of all personally identifiable information, the Bill's requirement of robust notice and opt-out consent for nonsensitive personally identifiable information improves on the level of notice and choice currently provided by many websites. Also, I support the permanence of consent provision found in Section 102(e), which essentially provides that a consumer's privacy preferences stay with the user despite corporate changes.

Section 103's requirement that changes in privacy policies or the existence of privacy breaches be communicated to consumers is particularly commendable. Many websites place the privacy protection burden on consumers to keep track of changes in a website's privacy policy. Section 103 appropriately places that responsibility on the internet service provider, online service provider, or operator of a commercial website. Likewise, the Bill's provision requiring user notification of material changes in the privacy policy allows consumers to utilize updated, relevant information when deciding how or whether to protect their own personal information. Section 103 illustrates the balanced approach of this Bill to the extent it acknowledges that there may be situations where delayed consumer notifications is appropriate.

The exceptions contained in Section 104 seem reasonable and again reflect the Bill's inherent respect for the need to balance the vital privacy interests of consumers with the economic and financial interests of e-business.

### *Access*

The access provision of Section 105 appropriately enables consumers to suggest corrections or deletions of personally, identifiable information that the provider or operator has collected or combined with personally identifiable information gathered from other sources. The reasonableness test incorporated in this section strikes an appropriate balance among the competing interests of consumer privacy, the relative sensitivity of different types of personal information, and the burdens and costs imposed on the website operator.

### *Security*

The security provision in Section 106 is consistent with the approach taken by the Commission in its Gramm-Leach-Bliley Act Security Rulemaking. Rather than dictate a one-size-fits-all solution, it is up to the website to establish and maintain reasonable procedures necessary to protect the security, confidentiality, and integrity of the data it maintains.

*Title II—Enforcement*

I am impressed with the range of remedies included under this Title, including the authority to impose civil penalties and establish redress funds for consumers for violations of Title I. In addition, this Title allows private rights of action as well as state actions.

*Title III—Application to Congress and Federal Agencies*

To my knowledge, the federal agencies do not trade in private consumer information for commercial purposes. Therefore, I see no justification for Section 302. However, I do believe that federal agencies should provide notice to consumers about their information collection practices consistent with applicable federal law.

*Title IV—Miscellaneous*

Section 402 provides that the effective date of the Act will be the day after the date the Commission publishes a final rule under Section 403. While I am pleased that there is no “grace period” for compliance with this Title, I am disappointed that data collectors will be free from liability for data they collected without consumer consent before the Act’s effective date. I also hope that Congress will resist obvious delaying tactics, such as proposals for additional studies.

*Technical concerns*

Section 403 may need technical modifications to achieve the Bill’s goals. Our staff would be pleased to assist you in these efforts. Specifically, Section 403 should reflect that the rulemaking contemplated by the Act is to be conducted pursuant to the Administrative Procedures Act rather than through a Magnuson Moss Rulemaking.

I appreciate the opportunity to express my views, and I hope they are helpful.

Sincerely,

SHEILA F. ANTHONY,  
*Commissioner.*

## CHANGES IN EXISTING LAW

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new material is printed in italic, existing law in which no change is proposed is shown in roman):

## COMMUNICATIONS ACT OF 1934

**SEC. 631. PROTECTION OF SUBSCRIBER PRIVACY.**

[47 U.S.C. 551]

(a) NOTICE TO SUBSCRIBER REGARDING PERSONALLY IDENTIFIABLE INFORMATION; DEFINITIONS.—

(1) At the time of entering into an agreement to provide any cable service or other service to a subscriber and at least once a year thereafter, a cable operator shall provide notice in the

form of a separate, written statement to such subscriber which clearly and conspicuously informs the subscriber of—

(A) the nature of personally identifiable information collected or to be collected with respect to the subscriber and the nature of the use of such information;

(B) the nature, frequency, and purpose of any disclosure which may be made of such information, including an identification of the types of persons to whom the disclosure may be made;

(C) the period during which such information will be maintained by the cable operator;

(D) the times and place at which the subscriber may have access to such information in accordance with subsection (d); and

(E) the limitations provided by this section with respect to the collection and disclosure of information by a cable operator and the right of the subscriber under subsections (f) and (h) to enforce such limitations.

In the case of subscribers who have entered into such an agreement before the effective date of this section, such notice shall be provided within 180 days of such date and at least once a year thereafter.

(2) For purposes of this section, other than subsection (h)—

(A) the term “personally identifiable information” does not include any record of aggregate data which does not identify particular persons;

(B) the term “other service” includes any wire or radio communications service provided using any of the facilities of a cable operator that are used in the provision of cable service; and

(C) the term “cable operator” includes, in addition to persons within the definition of cable operator in section 602, any person who (i) is owned or controlled by, or under common ownership or control with, a cable operator, and (ii) provides any wire or radio communications service.

(b) COLLECTION OF PERSONALLY IDENTIFIABLE INFORMATION USING CABLE SYSTEM.—

(1) Except as provided in paragraph (2), a cable operator shall not use the cable system to collect personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned.

(2) A cable operator may use the cable system to collect such information in order to—

(A) obtain information necessary to render a cable service or other service provided by the cable operator to the subscriber; or

(B) detect unauthorized reception of cable communications.

(c) DISCLOSURE OF PERSONALLY IDENTIFIABLE INFORMATION.—

(1) Except as provided in paragraph (2), a cable operator shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions

as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator.

(2) A cable operator may disclose such information if the disclosure is—

(A) necessary to render, or conduct a legitimate business activity related to, a cable service or other service provided by the cable operator to the subscriber;

(B) subject to subsection (h), made pursuant to a court order authorizing such disclosure, if the subscriber is notified of such order by the person to whom the order is directed;

(C) a disclosure of the names and addresses of subscribers to any cable service or other service, if—

(i) the cable operator has provided the subscriber the opportunity to prohibit or limit such disclosure, and

(ii) the disclosure does not reveal, directly or indirectly, the—

(I) extent of any viewing or other use by the subscriber of a cable service or other service provided by the cable operator, or

(II) the nature of any transaction made by the subscriber over the cable system of the cable operator; or

(D) to a government entity as authorized under chapters 119, 121, or 206 of title 18, United States Code, except that such disclosure shall not include records revealing cable subscriber selection of video programming from a cable operator.

(d) SUBSCRIBER ACCESS TO INFORMATION.—A cable subscriber shall be provided access to all personally identifiable information regarding that subscriber which is collected and maintained by a cable operator. Such information shall be made available to the subscriber at reasonable times and at a convenient place designated by such cable operator. A cable subscriber shall be provided reasonable opportunity to correct any error in such information.

(e) DESTRUCTION OF INFORMATION.—A cable operator shall destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information under subsection (d) or pursuant to a court order.

(f) CIVIL ACTION IN UNITED STATES DISTRICT COURT; DAMAGES; ATTORNEY'S FEES AND COSTS; NONEXCLUSIVE NATURE OF REMEDY.—

(1) Any person aggrieved by any act of a cable operator in violation of this section may bring a civil action in a United States district court.

(2) The court may award—

(A) actual damages but not less than liquidated damages computed at the rate of \$100 a day for each day of violation or \$1,000, whichever is higher;

(B) punitive damages; and

(C) reasonable attorneys' fees and other litigation costs reasonably incurred.

(3) The remedy provided by this section shall be in addition to any other lawful remedy available to a cable subscriber.

(g) REGULATION BY STATES OR FRANCHISING AUTHORITIES.—Nothing in this title shall be construed to prohibit any State or any franchising authority from enacting or enforcing laws consistent with this section for the protection of subscriber privacy.

(h) DISCLOSURE OF INFORMATION TO GOVERNMENTAL ENTITY PURSUANT TO COURT ORDER.—Except as provided in section (c)(2)(D), a governmental entity may obtain personally identifiable information concerning a cable subscriber pursuant to a court order only if, in the court proceeding relevant to such court order—

(1) such entity offers clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case; and

(2) the subject of the information is afforded the opportunity to appear and contest such entity's claim.

(i) APPLICATION OF ONLINE PERSONAL PRIVACY ACT.—*With respect to the provision by a cable operator of Internet service or on-line service and the operation by a cable operator of a commercial website, as such terms are defined in or under the Online Personal Privacy Act, the provisions of that Act shall apply in lieu of this section.*

## NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY ACT

### SEC. 20. COMPUTER STANDARDS PROGRAM.

[15 U.S.C. 278 G-3]

(a) DEVELOPMENT OF STANDARDS, GUIDELINES, METHODS, AND TECHNIQUES FOR COMPUTER SYSTEMS.—The Institute shall—

(1) have the mission of developing standards, guidelines, and associated methods and techniques for computer systems;

(2) except as described in paragraph (3) of this subsection (relating to security standards), develop uniform standards and guidelines for Federal computer systems, except those systems excluded by section 2315 of title 10, United States Code, or section 3502(9) of title 44, United States Code;

(3) have responsibility within the Federal Government for developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems except—

(A) those systems excluded by section 2315 of title 10, United States Code, or section 3502(9) of title 44, United States Code; and

(B) those systems which are protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy, the primary purpose of which standards and guidelines shall be to control loss and unauthorized modification or disclosure of

sensitive information in such systems and to prevent computer-related fraud and misuse;

(4) submit standards and guidelines developed pursuant to paragraphs (2) and (3) of this subsection, along with recommendations as to the extent to which these should be made compulsory and binding, to the Secretary of Commerce for promulgation under section 5131 of the Clinger-Cohen Act of 1996;

(5) develop guidelines for use by operators of Federal computer systems that contain sensitive information in training their employees in security awareness and accepted security practice, as required by section 5 of the Computer Security Act of 1987; and

(6) develop validation procedures for, and evaluate the effectiveness of, standards and guidelines developed pursuant to paragraphs (1), (2), and (3) of this subsection through research and liaison with other government and private agencies.

(b) TECHNICAL ASSISTANCE AND IMPLEMENTATION OF STANDARDS DEVELOPED.—In fulfilling subsection (a) of this section, the Institute is authorized—

(1) to assist the private sector, upon request, in using and applying the results of the programs and activities under this section;

(2) as requested, to provide to operators of Federal computer systems technical assistance in implementing the standards and guidelines promulgated pursuant to section 5131 of the Clinger-Cohen Act of 1996;

(3) to assist, as appropriate, the Office of Personnel Management in developing regulations pertaining to training, as required by section 5 of the Computer Security Act of 1987;

(4) to perform research and to conduct studies, as needed, to determine the nature and extent of the vulnerabilities of, and to devise techniques for the cost-effective security and privacy of sensitive information in Federal computer systems; and

(5) to coordinate closely with other agencies and offices (including, but not limited to, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, the Office of Technology Assessment, and the Office of Management and Budget)—

(A) to assure maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and

(B) to assure, to the maximum extent feasible, that standards developed pursuant to subsection (a)(3) and (5) are consistent and compatible with standards and procedures developed for the protection of information in Federal computer systems which is authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

(c) PROTECTION OF SENSITIVE INFORMATION.—For the purposes of—

(1) developing standards and guidelines for the protection of sensitive information in Federal computer systems under subsections (a)(1) and (a)(3), and

(2) performing research and conducting studies under subsection (b)(5), the Institute shall draw upon computer system technical security guidelines developed by the National Security Agency to the extent that the National Bureau of Standards determines that such guidelines are consistent with the requirements for protecting sensitive information in Federal computer systems.

*(d) DEVELOPMENT OF INTERNET PRIVACY PROGRAM.—The Institute shall encourage and support the development of one or more computer programs, protocols, or other software, such as the World Wide Web Consortium’s P3P program, capable of being installed on computers, or computer networks, with Internet access that would reflect the user’s preferences for protecting personally-identifiable or other sensitive, privacy-related information, and automatically execute the program, once activated, without requiring user intervention.*

**[(d)] (e) DEFINITIONS.—**As used in this section—

(1) the term “computer system”—

(A) means any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information; and

(B) includes—

- (i) computers;
- (ii) ancillary equipment;
- (iii) software, firmware, and similar procedures;
- (iv) services, including support services; and
- (v) related resources;

(2) the term “Federal computer system” means a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer system) on behalf of the Federal Government to accomplish a Federal function;

(3) the term “operator of a Federal computer system” means a Federal agency, contractor of a Federal agency, or other organization that processes information using a computer system on behalf of the Federal Government to accomplish a Federal function;

(4) the term “sensitive information” means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy; and

(5) the term "Federal agency" has the meaning given such term by section 3(b) of the Federal Property and Administrative Services Act of 1949.

