

# SELECTED RECENT PRIVACY INITIATIVES BY THE U.S. FEDERAL GOVERNMENT

SEPTEMBER 25, 2000

## I. Federal

**Protecting the privacy of individuals who access government resources electronically or whose sensitive data is in government files.**

1. Letter from Office of Management and Budget Office of Information and Regulatory Affairs Administrator John Spotila on the use of "cookies" on federal government web-sites. (September 5, 2000)  
<http://www.cio.gov/docs/OMBCookies2.htm>
2. Press release and Federal Register Notice announcing a study of the treatment of sensitive personal information in bankruptcy cases. (July 26, 2000)  
<http://www.usdoj.gov/ust/privacy/privacy.htm>
3. Office of Management and Budget Director Jacob J. Lew memorandum on privacy policies and data collection on websites. (June 22, 2000)  
<http://www.whitehouse.gov/omb/memoranda/m00-13.html>
4. IRS "privacy impact assessment," voted best practice by federal chief information officers. (February 25, 2000)  
<http://www.cio.gov/docs/IRS.htm>
5. Box on protecting personal privacy in proposed FY 2001 Federal Budget.  
<http://w3.access.gpo.gov/usbudget/fy2001/pdf/budget.pdf> (go to page 296)
6. OMB Director Lew memorandum on website policies. (June 2, 1999)  
<http://www.whitehouse.gov/omb/memoranda/m99-18.html>
7. President's memorandum on Privacy Act (May 14, 1998) and memorandum from OMB Director Lew.  
<http://www.whitehouse.gov/omb/memoranda/m99-05.html>

## II. Federal Trade Commission

**Privacy activities of the Federal Trade Commission.**

1. Link to various privacy initiatives of the FTC.  
<http://www.ftc.gov/privacy/index.html>

### III. Financial

#### Protecting the private, personal financial information of consumers.

1. Treasury Under-Secretary Gary Gensler testimony on personal financial privacy. (June 14, 2000)  
<http://www.house.gov/banking/61400gen.htm>
2. HR 4585. Administration financial privacy plan, as introduced in Congress. (May 6, 2000)  
<http://thomas.loc.gov/cgi-bin/query/C?c106:/temp/~c106wBaamP>
3. Clinton-Gore financial privacy plan outline. (April 30, 2000)  
<http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/2000/5/1/2.text.1>
4. Financial privacy press briefing. (April 30, 2000)  
<http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/2000/5/2/4.text.1>
5. President's remarks at Eastern Michigan University on plan to protect financial privacy. (April 30, 2000)  
<http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/2000/5/2/5.text.1>
6. President's remarks at the signing of financial modernization legislation. (November 12, 1999)  
<http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/1999/11/12/29.text.1>
7. Treasury Under-Secretary Gary Gensler testimony on personal financial protection. (July 21, 1999)  
<http://www.house.gov/banking/72199gen.htm>
8. President's speech on financial privacy protection. (May 4, 1999)  
<http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/1999/5/5/3.text.1>

### IV. General – Administration

#### Raising awareness of privacy issues in general and calling for an “Electronic Bill of Rights” for individuals.

1. Profile of the work of the Chief Counselor for Privacy by *USA Today*. (June 7, 2000)  
<http://www.usatoday.com/life/cyber/tech/cti036.htm>
2. Vice President's announcement on privacy issues. (July 31, 1998)  
<http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/1998/8/3/7.text.1>
3. Vice President's remarks at NYU announcing electronic bill of rights. (May 14, 1998)  
<http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/1998/5/14/7.text.1>

## V. Genetic

**A move to ban the use of genetic information in hiring decisions in the federal government, and a call to extend those important privacy safeguards to the private sector.**

1. Announcement by the President of executive order on genetic discrimination. (February 8, 2000)  
<http://www.pub.whitehouse.gov/uri-res/12R?urn:pdi://oma.eop.gov.us/2000/2/8/7.text.2>
2. Text of executive order. (February 8, 2000)  
<http://www.pub.whitehouse.gov/uri-res/12R?urn:pdi://oma.eop.gov.us/2000/2/8/8.text.2>
3. Fact sheet on the announcement of the executive order. (February 8, 2000)  
<http://www.pub.whitehouse.gov/uri-res/12R?urn:pdi://oma.eop.gov.us/2000/2/9/2.text.1>
4. Legislation supported by the Administration to ban genetic discrimination in the private sector. (July 1, 1999)  
<http://thomas.loc.gov/cgi-bin/query/C?c106:/temp/~c106uPWCK6>

## VI. Medical

**Writing rules to ensure that individuals' most personal medical information is not released without authorization.**

1. Testimony by Margaret A. Hamburg, Assistant Secretary for Planning and Evaluation, U.S. Department of Health and Human Services. (February 17, 2000)  
<http://waysandmeans.house.gov/health/106cong/2-17-00/2-17hamb.htm>
2. Proposed medical privacy rules. (November 3, 1999)  
[http://erm.aspe.hhs.gov/ora\\_web/plsql/erm\\_rule.library](http://erm.aspe.hhs.gov/ora_web/plsql/erm_rule.library)
3. Medical privacy rules announcement. (October 29, 1999)  
<http://www.pub.whitehouse.gov/uri-res/12R?urn:pdi://oma.eop.gov.us/1999/10/29/4.text.1>
4. President's remarks at the announcement. (October 29, 1999)  
<http://www.pub.whitehouse.gov/uri-res/12R?urn:pdi://oma.eop.gov.us/1999/10/29/6.text.1>
5. Announcement of Health and Human Services Secretary Donna Shalala's report, urging Congress to protect personal medical records. (September 11, 1997)  
<http://www.hhs.gov/news/press/1997pres/970911.html>
6. Text of Health and Human Services report. (September 11, 1997)  
<http://aspe.os.dhhs.gov/admsimp/pvcrec0.htm>

## VII. Online Privacy

### **Encouraging effective self-regulatory on-line privacy initiatives.**

1. Announcement of new self-regulatory code for on-line profiling (July 27, 2000)  
<http://204.193.246.62/public.nsf/docs/E4CED19B7B5783EB8525692900710A7B>
2. Network Advertising Initiative self-regulatory code text. (July 27, 2000)  
<http://www.networkadvertising.org/press/principles.pdf>
3. Commerce Secretary William Daley's statement on efforts to promote on-line privacy. (May 22, 2000)  
<http://osecm:13.osec.doc.gov/public.nsf/docs/FE72F69B4AAC3ABA852568E700776E90>
4. President's speech at Aspen Institute. (March 3, 2000)  
<http://www.pub.whitehouse.gov/uri-res/12R?urn:pdi://oma.eop.gov.us/2000/3/3/27.text.1>
5. Annual report on electronic commerce by the U.S. Government Working Group on Electronic Commerce. (1999)  
<http://www.ecommerce.gov/annrpt.htm>

## VIII. Online Security

### **Efforts to promote public safety in cyberspace, alongside individual privacy, and to update U.S. laws for the Internet Age.**

1. Fact sheet on Administration legislative proposal. (July 17, 2000)  
<http://www.pub.whitehouse.gov/uri-res/12R?urn:pdi://oma.eop.gov.us/2000/7/17/15.text.1>
2. Speech by White House Chief of Staff John Podesta. (July 17, 2000)  
<http://www.pub.whitehouse.gov/uri-res/12R?urn:pdi://oma.eop.gov.us/2000/7/18/4.text.1>
3. Clinton Administration legislative proposal on cyber-security.  
<http://thomas.loc.gov/home/c106query.html#billno> (search for bill S. 3083)
4. Memorandum by Office of Management and Budget Director Jacob J. Lew, "Incorporating and Funding Security in Information Systems Investments." (February 28, 2000)  
<http://www.whitehouse.gov/omb/memoranda/m00-07.html>
5. Cybersecurity Summit, with President's remarks. (February 15, 2000)  
<http://www.pub.whitehouse.gov/uri-res/12R?urn:pdi://oma.eop.gov.us/2000/2/15/2.text.1>

## IX. Privacy and Encryption

### **A new strategy to balance privacy, electronic commerce, and national security.**

1. Encryption announcement. (September 16, 1999)  
<http://www.pub.whitehouse.gov/uri-res/12R?urn:pdi://oma.eop.gov.us/1999/9/16/17.text.1>

2. Encryption press briefing. (September 16, 1999)  
<http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/1999/9/17/2.text.1>

## X. Safe Harbor

Provisions under which personal information may be transferred from the European Union to the United States.

1. Safe harbor principles. (June, 2000)  
<http://www.ita.doc.gov/td/ecom/SHPRINCIPLESFINAL.htm>
2. Frequently asked questions. (June, 2000)  
<http://www.ita.doc.gov/td/ecom/menu.html>
3. Safe Harbor statement by Commerce Secretary Bill Daley. (May 31, 2000)  
<http://oscentl3.oscc.doc.gov/public.nsf/docs/169C6EEE9A01CA64852568F00058DF37>

## XI. Social Security Numbers

Proposing legislation to protect individuals' Social Security numbers, a commonly used tool for identification purposes in the United States.

1. Vice President's announcement of the proposal. (June 8, 2000)  
<http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/2000/6/9/5.text.1>
2. Text of the legislation. (June 8, 2000)  
<http://thomas.loc.gov/cgi-bin/query/C?c106:/temp/~c106dj8x3g>



EXECUTIVE OFFICE OF THE PRESIDENT  
OFFICE OF MANAGEMENT AND BUDGET  
WASHINGTON, D.C. 20503

June 2, 1999

THE DIRECTOR

M99-18

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS  
AND AGENCIES

FROM:

Jacob J. Lew  
Director

A handwritten signature in black ink, appearing to read "Jacob J. Lew", written over the printed name and title.

SUBJECT:

Privacy Policies on Federal Web Sites

This memorandum directs Departments and Agencies to post clear privacy policies on World Wide Web sites, and provides guidance for doing so. As a first priority, you must post privacy policies to your Department or Agency's principal web site by September 1, 1999. By December 1, 1999, add privacy policies to any other known, major entry points to your sites as well as at any web page where you collect substantial personal information from the public. Each policy must clearly and concisely inform visitors to the site what information the agency collects about individuals, why the agency collects it, and how the agency will use it. Privacy policies must be clearly labeled and easily accessed when someone visits a web site.

Federal agencies must protect an individual's right to privacy when they collect personal information. This is required by the Privacy Act, 5 U.S.C. 552a, and OMB Circular No. A-130, "Management of Federal Information Resources," 61 Fed. Reg. 6428 (Feb. 20, 1996), and supported by the *Principles for Providing and Using Personal Information* published by the Information Infrastructure Task Force on June 6, 1995. Posting a privacy policy helps ensure that individuals have notice and choice about, and thus confidence in, how their personal information is handled when they use the Internet.

New information technologies offer exciting possibilities for improving the quality and efficiency of government service to the American people. Web sites are a powerful tool for conveying information on topics relating to activities, objectives, policies and programs of the Federal Government. Web pages provide a simple and speedy means of gaining access to information about the Government, thereby increasing knowledge and understanding of what Government is doing on the people's behalf. Looking ahead, as contemplated for instance by the Government Paperwork Elimination Act, people will conduct more and more business and other activities with the Government electronically. We cannot realize the full potential of the web until people are confident we protect their privacy when they visit our sites.

To assist Departments and Agencies in reviewing their existing privacy policy or in creating such a policy, I have attached guidance and model privacy language for several different information practices that may apply to your web sites. You can use the model language verbatim, or as a starting point in crafting a policy tailored to meet your own requirements and needs.

For any questions about this guidance, contact Peter P. Swire, Chief Counselor for Privacy, Office of Management and Budget, phone (202) 395-1095, fax (202) 395-5167, e-mail [Peter\\_Swire@omb.eop.gov](mailto:Peter_Swire@omb.eop.gov). To provide assistance to Agencies and Departments in implementing web privacy policies, Mr. Swire will form a Steering Committee for Federal Agency Privacy Policies.

Attachment

**June 1, 1999**

## **GUIDANCE AND MODEL LANGUAGE FOR FEDERAL WEB SITE PRIVACY POLICIES**

Every Federal web site must include a privacy policy statement, even if the site does not collect any information that results in creating a Privacy Act record. This statement tells the visitors to your site how you handle any information you get from them. Federal agency web sites are highly diverse, and have many different purposes. The privacy policies that agencies write for those sites are also diverse. Agencies must tailor their statements to the information practices of each individual site. It is important to post your site's policy promptly, so visitors to your site know the site's information practices.

This attachment provides guidance and model language on privacy statements. You can use this guidance and model language to help identify the issues that privacy policies must cover, draft the language, and get it approved. This will allow you to post your policies expeditiously.

Agencies have been carrying out reviews of their systems of records notices to implement the President's Memorandum of May 14, 1998. Agencies should have sent their reports on their reviews to OMB by May 14, 1999. If you have not already done so, at this time you should post a general privacy policy on your Department and Agency web sites. The statement should include a clear overall description of your privacy practices. Do NOT delay creating this privacy policy until you revise all your agency's systems of records.

This attachment provides a brief discussion of different information practices, followed where appropriate by one or more samples from existing federal web sites and by a URL for each of those samples. The discussion is based on analysis by the Steering Committee for Federal Agency Privacy Policies. The members of the committee are listed at the end of this attachment. The Steering Committee includes representatives of different parts of agencies that may play a role in creating web privacy policies, such as web masters, Chief Information Officers, General Counsels, Privacy Act officials, and designated privacy policy officials. You can contact members of the Steering Committee to talk about their experiences in creating privacy policies.

This document provides guidance on the following situations:

- (1) Introductory language.
- (2) Information collected and stored automatically.
- (3) Information collected from e-mails and web forms.
- (4) Security, intrusion, and detection language.
- (5) Significant actions where information may be subject to the Privacy Act.

## (1) Introductory language.

*Discussion:* Web sites are the front door for many contacts by individuals with the government. Having clear overview language about your privacy practices at the start of the policy can provide a helpful introduction to a web policy.

Web privacy policies can reassure individuals that information you collect about them when they visit your site will be well and appropriately handled. You should write such reassurances in plain English.

### *Sample One:*

"Thank you for visiting the White House Website and reviewing our privacy policy. Our privacy policy is clear: We will collect no personal information about you when you visit our website unless you choose to provide that information to us.

*Source:* [www.whitehouse.gov/WH/html/privacy.html](http://www.whitehouse.gov/WH/html/privacy.html).

### *Sample Two:*

"The privacy of our customers has always been of utmost importance to the Social Security Administration. In fact our first regulation, published in 1937, was written and published to ensure your privacy. Our concern for your privacy is no different in the electronic age.

Our Internet privacy policy is:

- You do not have to give us personal information to visit our site.
- We collect personally identifiable information (name, email address, Social Security number, or other unique identifier) only if specifically and knowingly provided by you.
- Personally identifying information you provide will be used only in connection with Social Security Online or for such other purposes as are described at the point of collection.
- Information is collected for statistical purposes and SSA sometimes performs analyses of user behavior in order to measure customer interest in the various areas of our site. We will disclose this information to third parties only in aggregate form.
- We do not give, sell or transfer any personal information to a third party.
- We do not enable "cookies." (A "cookie" is a file placed on your hard drive by a Web site that allows it to monitor your use of the site, usually without your knowledge.)

*Source:* [www.ssa.gov/privacy.html](http://www.ssa.gov/privacy.html)

## **(2) Information collected and stored automatically.**

*Discussion:* In the course of operating a web site, certain information may be collected automatically in logs or by cookies. Some agencies may be able to collect a great deal of information, but by policy elect to collect only limited information. In some instances, agencies may have the technical ability to collect information and later take additional steps to identify people, such as by looking up static Internet Protocol addresses that can be linked to specific individuals. Your policy should make clear whether or not you are collecting this type of information and whether you will take further steps to collect more information.

### *Sample One:*

#### **"Information Collected and Stored Automatically**

If you do nothing during your visit but browse through the website, read pages, or download information, we will gather and store certain information about your visit automatically. This information does not identify you personally. We automatically collect and store only the following information about your visit:

1. The Internet domain (for example, "xcompany.com" if you use a private Internet access account, or "yourschool.edu" if you connect from a university's domain) and IP address (an IP address is a number that is automatically assigned to your computer whenever you are surfing the Web) from which you access our website;
2. The type of browser and operating system used to access our site;
3. The date and time you access our site;
4. The pages you visit; and
5. If you linked to the White House website from another website, the address of that website.

We use this information to help us make our site more useful to visitors -- to learn about the number of visitors to our site and the types of technology our visitors use. We do not track or record information about individuals and their visits.

*Source:* [www.whitehouse.gov/WH/html/privacy.html](http://www.whitehouse.gov/WH/html/privacy.html).

### *Sample Two:*

"This is how we will handle information we learn about you from your visit to our website. The information we receive depends upon what you do when visiting our site.

If you visit our site to read or download information, such as consumer brochures or press releases:

We collect and store only the following information about you: the name of the domain from which you access the Internet (for example, aol.com, if you are connecting from an America Online account, or princeton.edu if you are connecting from Princeton University's domain); the date and time you access our site; and the Internet address of the website from which you linked directly to our site.

We use the information we collect to measure the number of visitors to the different sections of our site, and to help us make our site more useful to visitors.

Source: [www.ftc.gov/ftc/privacy1.htm](http://www.ftc.gov/ftc/privacy1.htm).

*Sample Three:*

"Example Information Collected for Statistical Purposes

Below is an example of the information collected based on a standard request for a World Wide Web document:

```
xxx.yyy.com -- [28/Jan/1997:00:00:01 -0500]
"GET /sitename/news/nr012797.html HTTP/1.0" 200 16704
Mozilla 3.0/www.altavista.digital.com
```

xxx.yyy.com (or 123.123.23.12) -- this is the host name (or IP address) associated with the requester (you as the visitor). In this case, (....com) the requester is coming from a commercial address. Depending on the requestor's method of network connection, the host name (or IP address) may or may not identify a specific computer. Connections via many Internet Service Providers assign different IP addresses for each session, so the host name identifies only the ISP. The host name (or IP address) will identify a specific computer if that computer has a fixed IP address.

[28/Jan/1997:00:00:01 -0500] -- this is the date and time of the request

"GET /sitename/news/nr012797.html HTTP/1.0" -- this is the location of the requested file

200 -- this is the status code - 200 is OK - the request was filled

16704 -- this is the size of the requested file in bytes

Mozilla 3.0 -- this identifies the type of browser software used to access the page, which indicates what design parameters to use in constructing the pages

www.altavista.digital.com -- this indicates the last site the person visited, which indicates how people find this site

Requests for other types of documents use similar information. No other user-identifying information is collected.

*Source:* [www.defenselink.mil/warning/example.html](http://www.defenselink.mil/warning/example.html)

### **(3) Information Collected from E-mails and Web Forms.**

*Discussion:* Many websites receive identifiable information from e-mails or web forms. Some statement is appropriate about how the identifiable information is treated when the individual provides it. One general and helpful comment is to say (when it is true) that you only use information included in an e-mail for the purposes provided and that the information will be destroyed after this purpose has been fulfilled.

*Sample One:*

The Federal Trade Commission has two levels of disclosure. On its principal privacy policy page, it states the following:

"If you identify yourself by sending an E-mail:

You also may decide to send us personally-identifying information, for example, in an electronic mail message containing a complaint. We use personally-identifying information from consumers in various ways to further our consumer protection and competition activities. Visit Talk to Us to learn what can happen to the information you provide us when you send us e-mail."

*Source:* [www.ftc.gov/ftc/privacy1.htm](http://www.ftc.gov/ftc/privacy1.htm).

The FTC then has the following disclosure at its "Talk to Us" link:

You can contact us by postal mail, telephone, or electronically, via an on-line form. Before you do, there are a few things you should know.

The material you submit may be seen by various people. We may enter the information you send into our electronic database, to share with our attorneys and investigators involved in law enforcement or public policy development. We may also share it with a wide variety of other government agencies enforcing consumer protection, competition, and other laws. You may be contacted by the FTC or any of those agencies. In other limited circumstances, including requests from Congress or private individuals, we may be required by law to disclose information you submit.

Also, e-mail is not necessarily secure against interception. If your communication is very sensitive, or includes personal information like your bank account, charge card, or social security number, you might want to send it by postal mail instead."

*Source:* [www.ftc.gov/ftc/talk\\_to\\_us.htm](http://www.ftc.gov/ftc/talk_to_us.htm).

#### **(4) Security, Intrusion, Detection Language.**

*Discussion:* Many webmasters use information collected on a site to detect potentially harmful intrusions and to take action once an intrusion is detected. In some situations, the policy of the agency may be not to collect personal information such as from IP logs. In the event of authorized law enforcement investigations, however, and pursuant to any required legal process, information from those logs and other sources may be used to help identify an individual.

##### *Sample One:*

The Department of Defense uses the following language to alert users that information may be collected for security purposes:

- "4. For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.
5. Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with National Archives and Records Administration guidelines.

6. Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act."

*Source:* [www.defenselink.mil/warning/warn-di.html](http://www.defenselink.mil/warning/warn-di.html).

*Sample Two:* Department of Justice Privacy and Security Notice:

"For SITE SECURITY purposes and to ensure that this service remains available to all users, this Government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

NOTICE: We will not obtain personally-identifying information about you when you visit our site, unless you choose to provide such information to us."

*Source:* [www.usdoj.gov/privacy-file.htm](http://www.usdoj.gov/privacy-file.htm)

#### **(5) Significant actions where information enters a System of Records.**

*Discussion:* To date, a large fraction of federal web pages have not collected significant amounts of identifiable information in ways that entered directly into systems of records covered by the Privacy Act. Looking ahead, a greater range of actions may take place based on information provided to web sites. Examples might include electronic commerce transactions or updating of information about eligibility for benefits.

In systems of records where traditional paper collections of information are supplemented or replaced by electronic forms offered through a web site, the rules of the Privacy Act continue to apply. For situations where a Privacy Act notice would be required in the paper-based world, the general principle is that the equivalent notice is required in the on-line world. Posting of the relevant Privacy Act notice on the web page or through a well-marked hyperlink would be appropriate.

Steering Committee for Federal Agency Privacy Policies

The Steering Committee has helped develop the guidance in this document, drawing on the diverse functional experience of its members. Its members are available for questions and comments on the development of agency web privacy policies.

Peter Swire (chair), Chief Counselor for Privacy, Office of Management and Budget, phone (202) 395-1095, e-mail Peter\_Swire@omb.eop.gov.

Roger Baker, Chief Information Officer, Department of Commerce, phone (202) 482-4797, e-mail rbaker@doc.gov.

John Bentivoglio, Chief Privacy Officer, Department of Justice, phone (202) 514-2707, e-mail john.t.bentivoglio@usdoj.gov.

Ruth Doerflein, Internet/Intranet Program Manager, Department of Health and Human Services, phone (202) 690-5709, e-mail rdoerfle@~~us~~dhhs.gov.

Peggy Irving, Director, Office of the Privacy Advocate, Internal Revenue Service, phone (202) 783-7755, e-mail peggy.a.irving@m1.irs.gov (note: the number "1" follows @m).

Vahan Moushegian, Jr., Director, Defense Privacy Office, Department of Defense, phone (703) 607-2943, e-mail Vahan.Moushegian@osd.pentagon.mil.

Andy Pincus, General Counsel, Department of Commerce, phone (202) 482-4772, e-mail apincus@doc.gov.

The following two persons from the Federal Trade Commission are not members of the Steering Committee. They have worked with privacy policies for both the public and private sector, however, and have offered to be available for questions from those working on agency policies:

Martha Landesberg, attorney, Federal Trade Commission, phone (202) 326-2825, e-mail mlandesberg@ftc.gov.

David Medine, Associate Director for Financial Practices, Federal Trade Commission, phone (202) 326-3025, e-mail dmedine@ftc.gov.

**STATEMENT OF**

**JOHN T. SPOTILA**

**ADMINISTRATOR, OFFICE OF INFORMATION AND REGULATORY AFFAIRS  
OFFICE OF MANAGEMENT AND BUDGET**

**SUBMITTED TO**

**THE SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,  
INFORMATION, AND TECHNOLOGY**

**COMMITTEE ON GOVERNMENT REFORM**

**UNITED STATES HOUSE OF REPRESENTATIVES**

**MAY 15, 2000**

Mr. Chairman and members of the Committee, thank you for inviting me here to present the Administration's views on H.R. 4049, the "Privacy Commission Act." As Administrator of OMB's Office of Information and Regulatory Affairs, I care deeply about the protection of privacy. In 1998, OIRA took on enhanced responsibility for coordinating privacy policy throughout the Administration. OIRA already had policy responsibility under the Privacy Act of 1974, which applies to federal government systems of records. Now it plays a central coordinating role for privacy policy more generally. Last year, OMB appointed its first Chief Counselor for Privacy, Peter Swire, to be the point person in this coordination effort. Peter is with me here today.

The President and the Vice President are committed to the protection of individual privacy. As President Clinton said on April 30, when announcing his new financial privacy proposal: "From our earliest days, part of what has made America unique has been our dedication to freedom, and the clear understanding that real freedom requires a certain space of personal privacy." Vice President Gore showed similar leadership in 1998 when he called for an Electronic Bill of Rights, emphasizing that we should all do our part to protect individual privacy, relying on private sector leadership where possible, on legislation when necessary, on responsible government handling of personal information, and on an informed public.

In studying the proposed findings for H.R. 4049, we find much common ground. We agree that Americans are increasingly concerned about the security and use of their personal information. We agree that the shift from an industry-focused economy to an information-focused economy calls for reassessing the way we balance personal privacy and information use. As Administrator of OIRA, I work extensively on information policy issues relating to computer security, privacy, information collection, and our transition to the electronic delivery of government services. In these and other areas, we are working hard to gain the advantages that

come from new technologies while guarding against possible costs to privacy and security that can come from badly crafted uses of those technologies.

In some areas, we already know that we must act swiftly to protect privacy and security. Indeed, the Administration's biggest concern with H.R. 4049 is the risk that some might use the Commission as a reason to delay much-needed privacy legislation. We understand that supporters of H.R. 4049 have emphasized that it should not be used as a reason for delay. But we are also aware from public reports that those who oppose privacy reform would prefer to have Congress study the issue indefinitely rather than take action. In the Administration's view, such delay would be unwise. We cannot afford to take a year and a half off in protecting Americans' privacy. We believe that action is needed now in the areas of financial privacy, medical records privacy, and genetic discrimination.

Before addressing specific aspects of H.R. 4049, it would be useful to review recent federal privacy initiatives.

### Overview

There have been extensive initiatives by the Federal government since 1993 to study and take appropriate action in the area of privacy protection. Study of privacy was an integral part of the National Information Infrastructure project, sometimes called the "information superhighway" effort, with the issuance in 1995 by an inter-agency Privacy Working Group of "Principles for Providing and Using Personal Information." (See: Privacy Working Group of the Information Infrastructure Task Force, [www.iitf.nist.gov/ipc/ipc-pub.html](http://www.iitf.nist.gov/ipc/ipc-pub.html).) This effort was led by OIRA. With Administration support, Congress has passed privacy legislation including the Drivers' Privacy Protection Act of 1994 (motor vehicle records), the Telecommunications Act of 1996 (authority for the Customer Proprietary Network Information regulations), the Health Insurance Portability and Accountability Act of 1996 (authority for the currently proposed medical privacy regulations), the Children's Online Privacy Protection Act of 1998 (children's online records), the Identify Theft and Assumption Deterrence Act of 1998 (deterrence of identity theft), and the Gramm-Leach-Bliley Act of 1999 (financial records).

In the online world, the Administration has encouraged self-regulatory efforts by industry. For especially sensitive information -- such as medical, financial, and children's online records -- legal protections are required. Recent activities have included:

- When children go online, parents should give their consent before companies gather personal information. Websites aimed at children must get such consent under the Children's Online Privacy Protection Act of 1998 and accompanying rules that went into effect in April of this year.
- The Department of Commerce, the Federal Trade Commission, the White House Electronic Commerce Working Group, and other parts of the Federal government

have undertaken a wide array of studies, reports, workshops, and other activities to address issues of online privacy. As one example, a public workshop last fall challenged the industry to address concerns about "online profiling," in which companies collect data, in ways few people would suspect, about individuals surfing the Internet.

- In the international sphere, the Department of Commerce has taken the lead in creating "safe harbor" principles for transfers of personal information between the European Union and the United States. These principles, to which the European Commission has now agreed, recognize the appropriateness of effective self-regulatory regimes. In developing the principles, the Department has sought public comment on four separate occasions.
- The President signed the Identity Theft and Assumption Deterrence Act of 1998. This March, the Department of the Treasury hosted an Identity Theft Summit to assist in the prevention, detection, and remediation of the significant problem of malicious misuse of another person's personal information for fraudulent purposes.
- The Administration continues to build privacy protections into its own activities. Last year, for instance, all Federal agencies successfully posted clear privacy policies on their websites. Programs are now underway to strengthen Government computer security to provide new privacy safeguards for personal information held by the Government. The new Privacy Subcommittee of the Chief Information Officers Council is undertaking initiatives to ensure that privacy is effectively built into government information technology systems.

#### Financial records.

Congress discussed financial privacy intensively in the course of its financial modernization debate last year. As the President pointed out when signing the law, the modernization law took significant steps to protect the privacy of financial transactions, but did not go far enough. The President asked OMB, the Department of Treasury, and the National Economic Council to craft a legislative proposal to close loopholes under existing law. On April 30, he announced his plan to protect consumers' financial privacy. This plan would include:

- Consumer choice: Giving consumers the right to choose whether a firm can share consumer financial information with third parties or affiliated firms.
- Enhanced protection for especially sensitive information: Requiring that a consumer give affirmative consent before a firm can gain access to medical information within the financial conglomerate, or share detailed information about a consumer's personal spending habits.

- Access and correction: Giving consumers a new right to review their information and correct material errors.
- Effective enforcement: Providing effective enforcement tools for financial institutions subject to Federal Trade Commission enforcement of privacy rules.
- Comparison shop on privacy policies: Giving consumers privacy notices upon application or request so they know how information is protected before a customer relationship is established.

These provisions were introduced in the House as H.R. 4380, attracting immediate and substantial support in both the House and the Senate. As Secretary of the Treasury Lawrence Summers emphasized on March 7, "It's time to start now."

### Medical Records

There has been a longstanding appreciation in the United States that individual medical records include especially sensitive information. Disclosing medical data can reveal what is happening inside a person's body, such as a report that a person is HIV positive, or inside a person's mind, such as the transcript of a session with a psychotherapist. The Federal government has recognized these concerns at least since 1973, when the Department of Health, Education, and Welfare first announced the basic fair information practices that underlie privacy policy today.

Congress recognized the need for legal protection of medical records when it passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA). After extensive discussions with stakeholders and as required by HIPAA, the Secretary of Health and Human Services issued her recommendations for health privacy legislation in September 1997. Congress was unable to meet the HIPAA deadline for enacting comprehensive privacy legislation by August 21, 1999. Accordingly, the President and Secretary Shalala announced proposed privacy regulations on October 29 of last year. It was HHS's goal to make the regulation process open to those who wanted to communicate their concerns in person. HHS met with many individuals and organizations to hear their concerns and clarify provisions of the proposed rule. HHS received over 53,000 submissions of comments by the February 17, 2000 deadline. HHS is now considering those comments, and the regulations will become final this year.

Although the medical privacy regulations will become final this year, there is a pressing need for further Congressional action. As HHS Assistant Secretary Margaret Hamburg testified in February of this year: "Health information privacy is a top priority for the Department and the Administration, and we continue to believe that legislation is the only way to achieve the goal." President Clinton explained some of the reasons for legislation when he proposed the privacy

regulations last October. The Administration is especially concerned that the enforcement powers under current law are not as effective as they should be. We recommend federal legislation that would allow punishment of those who misuse personal health information and redress for people who are harmed by its misuse. Administration officials have testified often on what should be included in medical privacy legislation, and we urge that there be no delay on this subject.

### Genetic Discrimination.

This February 8, President Clinton signed an executive order that prohibits every federal department and agency from using genetic information in any hiring or promotion action. This order ensures that critical health information from genetic tests not be used against federal employees. The President has also endorsed the Genetic Nondiscrimination in Health Insurance and Employment Act of 1999, introduced by Senator Daschle and Congresswoman Slaughter, which would extend these protections to the private sector and to individuals purchasing health insurance. As with financial and medical privacy, legislation is before the Congress to address especially sensitive personal data -- genetic information on individuals. The time to act on each of these issues is now.

\* \* \* \*

Let me turn now to the specifics of H.R. 4049.

### The Scope and Structure of the Proposed Commission.

As indicated earlier, the Administration has significant concerns that the Study Commission might be used by some as an excuse for delaying needed activity in privacy protection. These concerns are especially acute for topics such as medical, financial, and genetic information where good legislative proposals are before the Congress now. There has already been extensive discussion of these proposals within the Congress and among the stakeholders. Further study of these topics by the Commission would duplicate the public examination that has already taken place, without adding real value. The proposed medical privacy rules that become final this year will be the result of a multi-year process that generated over 53,000 public comments, many in extensive detail. These comments show a need for further action, not further study.

We recognize that the Congress needs to make its own judgments on these matters, and we defer to it in its assessment of what it needs to inform those judgments. It seems sensible, however, to adopt a focused approach to exploring these topics. Ideally, any further study efforts should be done within a short time frame and would build on, not duplicate, existing studies.

If there were to be a Commission, contrary to our recommendation, we should ensure that it focuses its efforts in an effective way. Again, we are concerned about potential delay. Casting too broad a net would delay the work of any new Commission, with uncertain results. We note,

for example, that the treatment of data collected on-line has been the subject of extensive hearings in Congress, as well as public workshops, public comments, studies, and reports by the Department of Commerce and the White House Electronic Commerce Working Group. The Federal Trade Commission is about to issue a major report. We recognize that this is a complicated area that requires careful evaluation and an understanding of new technology. It is not clear, however, that a Commission lasting 18 months will give decisionmakers the help they need.

Indeed, rather than have a Commission pursuing a very broad set of topics, it might be more productive to have technology and policy experts address specific, emerging issues that have not yet benefitted from much attention. One targeted way to study such privacy issues might be to enlist the expertise of the National Academy of Sciences/National Research Council or other appropriate bodies. The NAS/NRC has extensive experience in creating blue-ribbon groups with the expertise to provide insight into difficult policy problems. In the privacy area, the NAS/NRC has already produced studies such as "Cryptography's Role in Securing the Information Society" (1996) and "For the Record: Protecting Electronic Health Information" (1997). Perhaps we should call on it again.

The NAS/NRC's Computer Science and Telecommunications Board is currently exploring funding for a study on "Authentication Technologies and Their Privacy Implications." The problem identified for this study arises from the need to identify people in a trustworthy way--that is, to authenticate people--in order to facilitate business and other activities over the Internet. Many of the possible ways to identify people have privacy implications since they involve individuals turning over a good deal of personal information -- from a mother's maiden name to credit card numbers or other information that could put an individual at risk if revealed to unauthorized persons. As technology develops, our society needs to understand how to make authentication work in a way consistent with preserving privacy.

Another useful study topic, which similarly does not require a Commission, could be biometrics and privacy. "Biometrics" refer to fingerprints, iris scans, and other physical indicators of identity. Since many companies are now exploring the commercial deployment of biometric technology, now is a good time to assess the public policy of biometrics and privacy. If deployed carefully, biometrics could protect privacy by placing less reliance on sending credit card numbers or other sensitive information over the Internet. If deployed badly, however, biometric technology could create new privacy risks, such as if biometrics were used to record each room an employee enters while on the job. A study of this subject, taking proper account of new technological developments, could increase the likelihood that biometric systems will be more sensitive to privacy concerns as they become widely used.

For all these reasons, we believe there are sound alternatives to a Privacy Commission. If, nonetheless, legislation creating such a Commission moves forward, then we have specific concerns about certain provisions in H.R. 4049. For instance, as with other commissions on many important national issues, the President should have a greater role in appointing

Commission members. In addition, the current section 7(c) is objectionable because it could be interpreted as requiring Executive Branch agencies to turn over confidential or classified information to the proposed Commission. The text could read that agencies "may," rather than "shall" furnish that information.

As I emphasized earlier, we share with the Congress a very strong interest in protecting privacy and look forward to working with you to find suitable new ways to improve that protection. We understand the good intentions motivating the Congressional sponsors of H.R. 4049. Despite our reservations about the specifics of this bill, we welcome the commitment to privacy protection that they seek to demonstrate.

Mr. Chairman and Members of the Committee, thank you once again for the invitation to discuss these issues.

**STATEMENT FOR THE RECORD**

**JOHN T. SPOTILA**

**ADMINISTRATOR, OFFICE OF INFORMATION AND REGULATORY AFFAIRS**

**SUBMITTED TO**

**THE SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,  
INFORMATION, AND TECHNOLOGY**

**COMMITTEE ON GOVERNMENT REFORM**

**UNITED STATES HOUSE OF REPRESENTATIVES**

**18 MAY 2000**

**Mr. Chairman:**

Thank you for inviting me to provide the Administration's views with respect to H.R. 220, the "The Freedom and Privacy Restoration Act." We appreciate the opportunity to share our thoughts on this legislation.

President Clinton and Vice President Gore strongly support efforts to safeguard individual privacy. As the President said on April 30, when announcing his new financial privacy proposal: "From our earliest days, part of what has made America unique has been our dedication to freedom, and the clear understanding that real freedom requires a certain space of personal privacy." Vice President Gore showed similar leadership in 1998 when he called for an Electronic Bill of Rights, emphasizing that we should all do our part to protect individual privacy, relying on private sector leadership where possible, on legislation when necessary, on responsible government handling of personal information, and on an informed public.

With this direction, the Clinton Administration is engaged in many initiatives to protect personal privacy. For example, the Department of Health and Human Services is working on significant rules to protect the privacy of patients' medical records. We have also supported enhanced legal protections for financial records, as announced by President Clinton only two weeks ago.

The Administration is committed to protecting the privacy of personal information held by the government. For example, this February 8, President Clinton signed an executive order that prohibits every federal department and agency from using genetic information in any hiring or promotion action. This order ensures that critical health information from genetic tests not be used against federal employees. In addition, programs are underway to strengthen Government computer security to provide new privacy safeguards for personal information held by the Government.

As the Administrator of OIRA, I am especially pleased that OIRA in 1998 took on enhanced responsibility for coordinating privacy policy throughout the Administration. OIRA already had policy responsibility under the Privacy Act of 1974, which applies to federal government systems of records. Now it plays a central coordinating role for privacy policy more generally. Last year, OMB appointed its first Chief Counselor for Privacy to be the point person in this coordination effort. One of the first functions of the Chief Counselor was to ensure that all Federal agencies successfully posted clear privacy policies on their websites. We accomplished that goal in less than 4 months.

With respect to social security numbers, we agree that it is imperative for the government to handle such information with the utmost sensitivity. The Privacy Act of 1974 provides important protections against the misuse of an individual's personal information, including social security numbers.

- Under this Act, an agency may only disclose personal information with the individual's affirmative consent, subject to limited exceptions specified in the Act. Among these exceptions are disclosure: for intra-agency use, limited to people who need the information for the performance of their duties; pursuant to court order; and for statistical research purposes in form that does not identify the individual.
- The Act requires that individuals, at the time their information is collected, receive notice of the purposes for which the information will be used.
- The Act incorporates an important minimization principle – an agency may only maintain records about an individual that are relevant and necessary to accomplish a purpose required of the agency under a statute or executive order.
- Under the Act, an individual has a right to an accounting as to whom his or her records have been disclosed, when, and for what purpose.
- Under the Computer Matching and Privacy Protection Act of 1988 (CMPPA), an amendment to the Privacy Act, agencies must enter into an agreement with one another specifying how any computer data exchanged will be used and how it will be safeguarded. Under the CMPPA, individuals have the right to refute adverse information before having a benefit denied or terminated. The CMPPA also requires each agency to establish a Data Integrity Board to oversee matching activities.

The Privacy Act has special legal protections regarding the collection of social security numbers. It prohibits any federal, state, or local government agency from denying any individual a right, benefit, or privilege provided by law because of his or her refusal to disclose his or her social security number unless the disclosure is required by a Federal statute or covered by a grandfathering clause for certain pre-1975 activities. Moreover, any agency that requests such disclosure must inform the individual about whether the disclosure is mandatory or voluntary, by what authority, and what uses will be made of it.

The federal government does not sell social security numbers. It is sensitive to their confidentiality. Indeed, exemption 6 to the Freedom of Information Act (FOIA) protects social

security numbers from disclosure when FOIA requests are made.

The Administration shares the Committee's concern that the improper disclosure of social security numbers can cause significant problems, including the risk of identity theft -- a serious crime of increasing incidence. One of our top priorities was the passage of strong identity theft legislation and we applaud Congress for enacting the Identity Theft Assumption and Deterrence Act of 1998. More recently, at the President's request, the Department of Treasury convened a National Summit on Identity Theft on March 15 and 16 of this year. This Summit brought together private sector companies, public interest groups, and government agencies to consider concrete initiatives to address this crime.

Our sense is that particular threats to privacy in this area are arising in the private sector. Commercial use of the social security number for identification purposes has become much more widespread. Social security numbers are used in processing applications to college, for commercial loans, and in countless other areas. This is an area that warrants more attention.

We agree that we must all work diligently to prevent the misuse of social security numbers in all areas, including government. We believe, however, that the approach taken in H.R. 220 could pose great risks to the government's ability to serve the American people. We understand that other agencies are submitting views to the Committee describing the adverse impact of this bill on their individual operations. We thought it important to emphasize the bill's potentially harmful effects in at least three crosscutting areas: (1) the ability to deliver benefits to the public; (2) the ability to use statistical programs to help direct federal funds; and (3) the ability to root out fraud and abuse through matching programs.

The government needs social security numbers to deliver benefits and services to American citizens. Prohibiting the use of a social security number and the inter-agency use of any identifier, as H.R. 220 proposes to do, would hamper our ability to serve the public. Thus, the Department of Veterans Affairs (VA) relies upon social security numbers to coordinate patient care across the various public and private entities that currently provide care to veterans. Consider also the approximately 2.6 million members of the armed forces who upon separation or discharge are eligible for benefits administered by the VA. VA and the Department of Defense (DOD) clearly must work together to ensure that the benefits paid by VA are paid to the correct former DOD armed service member in the correct amount. Social security numbers provide the identifying information that is necessary for such an assurance. Similarly, in disaster relief cases, the Federal Emergency Management Association and the Small Business Administration rely upon social security numbers to identify disaster victims and determine eligibility for needed housing, individual and family assistance, and disaster loans. Likewise, the unemployment compensation program depends upon the use of social security numbers to assure proper payments of benefits to jobless workers.

Under H.R. 220, these agencies would evidently need to use other agency-specific identifiers to ensure that the right beneficiary is paid the right amount. To authenticate the identity of each individual before assigning such a number, the agency would presumably need to use address, telephone, mother's maiden name, and/or other verifying information. Such data can be unreliable for identification, however, because it is easy to falsify. To be more reliable, an

agency might need to collect and compare more than one data element. Even so, the approach would be unreliable and would require additional time and resources. It may be that new technologies -- such as digital signatures as part of a public key infrastructure -- will eventually ease the government and private sector burden in authenticating the identity of individuals. Currently, agencies often lack this capability.

Social security numbers are also critical in carrying out many statistical programs that generate our Nation's key social and economic indicators. We have worked diligently to improve the efficiency and quality of our statistical system and to reduce the reporting burden on individuals and businesses. With your help, we have also endeavored to create and promote necessary safeguards to ensure confidentiality protection for information that is acquired exclusively for statistical purposes. Our ability to provide high quality statistics for national, state, and local decision making would be severely hampered by a prohibition on the linking of social security numbers to data for statistical purposes. The Census Bureau's Intercensal Population Estimates Program is one example of the losses in quality and efficiency that would result. The production of intercensal population estimates relies on the effective use of administrative records that contain social security numbers, and the ability to link those records across time and across various administrative sources of information. By law, the Census Bureau must produce annual estimates of the population and its characteristics. As with all other census information, these data cannot be released in individually identifiable form. These data are used extensively to allocate federal funds for such other important purposes as distributing state and local government services, planning utility services, and locating retail and manufacturing establishments. The inability to use social security numbers and the associated inability to link birth records, death records, and similar administrative data would require a total redesign of the Intercensal Population Estimates Program. Recent evaluations indicate that alternative methods would result in estimates that are less accurate and less timely than those currently produced. Thus, the quality of statistical data and the efficiency of producing this critical information would be seriously eroded.

Social security numbers are also a critical component in the federal government's efforts to eliminate fraud and abuse. For example, in one program, the Department of Education matches files of student loan defaulters via name and social security number with records held by HHS's Office of Child Support enforcement showing current home address, employment address and income. This match enables Education to contact the delinquent debtors through current address information, attempt to secure voluntary repayment and, as a last resort, garnish their wages to pay off the debt, provided their wages exceed a certain threshold. Our estimates predict that this program will save taxpayers approximately \$1 billion over five years. In addition, the Department of Education and IRS currently have an income verification system for student loan borrowers who choose the Income Contingent Repayment (ICR) option. Under this option, the monthly payment amount is based on how much money the borrower earns after the borrower finishes his education. Education matches its data with IRS data -- again via name and social security number -- to determine how much a borrower's monthly payment should be. A third anti-fraud example is the use of the social security numbers to reduce improper payments in Medicare -- specifically by determining if Medicare beneficiaries should first be drawing on employer-sponsored insurance. This match depends on social security numbers to link spouses together and to determine the beneficiaries' employers.

We believe that current law protects well against the misuse of social security numbers by government agencies. We also have concerns that H.R. 220 would significantly impair our ability to deliver benefits and services to the American people, to perform important statistical and research functions, and to eradicate fraud and error in federal payment programs. While we understand the good intentions of the cosponsors and share their strong commitment to the protection of individual privacy, we urge great caution with H.R. 220, lest it cause unintended adverse consequences that we would all regret.

Thank you for the opportunity to present our views. Please do not hesitate to call upon us if we may be of additional assistance.

**STATEMENT OF**

**SALLY KATZEN**

**DEPUTY DIRECTOR FOR MANAGEMENT  
OFFICE OF MANAGEMENT AND BUDGET**

**SUBMITTED TO**

**THE SUBCOMMITTEE ON TELECOMMUNICATIONS, TRADE,  
AND CONSUMER PROTECTION**

**COMMITTEE ON COMMERCE**

**UNITED STATES HOUSE OF REPRESENTATIVES**

**OCTOBER 11, 2000**

Mr. Chairman and members of the Committee, I thank you for inviting me here today to discuss the important topic of privacy on government web-sites. As you know, protecting the privacy of American citizens is a very high priority for this Administration. We have worked hard to ensure that fundamental privacy protections are properly safeguarded as our government, and society at large, moves into the Digital Age. Nowhere is this task more important than in the federal government's obligation to continue to protect the privacy and confidentiality of the personal information that it maintains, and, now, to protect the privacy of individuals in their interactions with the government over the Internet.

Today the federal government is increasingly becoming an electronic government, full of new opportunities to provide services and information to the public quickly, easily, and when the public wants them. But as you, Mr. Chairman, and so many others here have noted, we must be vigilant to

ensure that personal privacy protections remain constant or are improved in the process of this transformation. I am proud to be able to testify today about the success of this Administration in meeting this challenge -- in taking major steps to boost the level of privacy afforded to American citizens when they access the government electronically. Without doubt, we have more to learn as a government. In this time of revolutionary changes in technology and information flows, all organizations do, no matter their size. But I am confident that we have achieved significant progress, and are clearly heading in the right direction in this critical area.

To understand the recent General Accounting Office reports on the privacy practices of federal agencies on-line, it is helpful to put them in their proper context and history. First, there is the Privacy Act of 1974, which for over a quarter of a century has afforded Americans strong legal protections for personal information stored in government systems of records -- no matter if they exist in paper or electronic form. These protections include notice, prohibitions on the unauthorized release of your personal information, the ability to access your own records, the ability to change errors in your records, and security safeguards, among other protections.

While this Act provides the bedrock privacy protections for Americans in their relations with the government, changes in technology -- most notably the dramatic increase in Internet-access to the government -- have produced a different world than existed in 1974. To keep current with meaningful privacy protections, the Office of Management and Budget has augmented the Privacy Act provisions with policy guidance, and the agencies' response, I believe, has been outstanding.

For example, in April 1999, a study revealed that just over one-third of federal agencies had privacy policies clearly posted on their main web pages. In June 1999, OMB Director Jacob J. Lew issued a memorandum to all agency heads directing them to post clearly labeled and clearly written privacy policies on their web-sites by September 1, 1999. Director Lew told agencies then, "We cannot realize the full potential of the web until people are confident we protect their privacy when they visit our sites."

The message was received by federal agencies. The General Accounting Office confirmed this result in a review conducted in April of 2000 and released on September 5, 2000 ("the first GAO report"). This GAO study found that 69 of 70 principal agency web-sites had a privacy policy posted on their sites -- and all 70 did within days of the report's release. Even more impressive, the GAO identified 2,692 major Web-site points of entry to six federal government agencies. These are sites where the largest number of citizens interact with the Federal government. Of the sites they reviewed, GAO found that only nine lacked privacy policies.

This record of progress is impressive, and, I believe, it is an accurate picture of the state of Federal privacy policies on-line. It is a story of working rapidly, across the expansive federal government and across thousands of web-pages, to ensure that citizens' privacy is protected when they choose to visit the federal government over the Internet.

As part of our continuing efforts in the area, OMB Director Lew issued another memorandum

this June to further enhance privacy protections on federal web-sites. Director Lew directed that cookies will not be used on Federal web-sites, except under very limited conditions. He also made clear, as a matter of Federal policy, that agencies are to comply with the standards of the Children's Online Privacy Protection Act, even though Congress did not include the Federal Government within the scope of that law. In addition, he directed each agency to describe its privacy practices and the steps taken to comply with Administration privacy policies in its budget submissions this fall to OMB. In this way, good privacy protection gets built into the budget process, emphasizing to everyone in the Government the importance of assuring citizen privacy.

These efforts to boost privacy safeguards have extended to areas beyond the federal government's practices on-line, as the Administration has supported strengthening citizens' legal privacy protections in such areas as medical information, financial records, genetic information, and Social Security numbers. These are categories of sensitive data that require protection in both the public and private sectors.

In light of this record of significant achievement, you may well ask why GAO reached the conclusions that it did about the Federal agencies' compliance with the fair information practices written by the Federal Trade Commission for commercial web-sites (the second GAO report). The answer, I believe, has more to do with the questions that were asked than the practices reported. Specifically, the Administration pointed out to GAO staff in the course of that study that the study was misdirected and that the answers to the study's questions would be misleading. GAO also has reported that the

FTC independently expressed concern that its methodology was "inappropriate for use in evaluating federal web site privacy policies."

The central premise of this particular study was apparently that the FTC formulation of fair information practices for commercial web-sites could appropriately be used to measure the privacy protections of government web-sites. We think it cannot. As noted, the FTC practices were designed for the private sector, where the Privacy Act and OMB policy do *not* apply. This is an important difference between commercial companies and federal agencies, even though both the government and businesses often use web-sites for the same core purposes: to provide information to consumers and to provide services to the public. The fact that there is no law establishing privacy protections for individuals in the commercial arena led the FTC to stress the need for those web-sites to make clear statements as to their privacy protections. The FTC does the same -- that is, require clear statements - - about commercial web-site policies with respect to access and security practices. It is through these statements that these companies can be held accountable.

Government web-sites, by contrast, do not have to make any representations to be held accountable. The Privacy Act establishes -- in the most public way possible -- the standards to which citizens can hold federal agencies accountable and exactly how they can hold agencies accountable. Thus, the test of whether a federal web-site provides privacy protection is not whether it includes statements that make it compatible with commercial practices, but rather whether good privacy protections are in place. The first GAO report confirmed that they are: When government web-sites

were measured against government privacy standards, the results were impressive.

In this Information Age, it is critical that the federal government continues to use technology to keep the public informed and to provide services for the public. The launch of the Federal government's FirstGov web-site on September 22 was a major step to enable easy access to government resources on-line. In this and many other ways, the need for privacy protection on-line – and the need for public confidence in the Federal government's on-line privacy standards – is expected to only increase in the years ahead. It would be most unfortunate if any misleading conclusions as to the state of privacy on federal web-sites interfered with our common goal of achieving an electronic government with full public participation.

As I said before, the federal government can, and should, continue to improve in its protection of the privacy of those individuals who access government web-sites. The first GAO report pointed out that we could do a better job of posting privacy policies at specific Federal web pages where a substantial amount of personal information is collected. That report also made recommendations about how OMB might provide clearer guidance to agencies, and we are working with the Federal CIO Council to respond to those recommendations. Beyond that, I think that we will learn much from the privacy materials included with the agency FY 2002 budget submissions to OMB. At the same time, I would again emphasize that the Administration's record on privacy protection in this area is strong, with a resolute commitment to safeguard personal privacy.

I thank you, Mr. Chairman, for holding this hearing today and for inviting me to testify. I look forward to continuing to work with you and the other members of this committee in making the federal government a model of good privacy practices.