M-99-18, Attachment

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

M-99-18 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/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

(**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/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.

Sample Three:
"Example Information Collected for Statistical Purpose/p>

> 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

(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.

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.

(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 Infrastructure Protection Act."

Source: www.defenselink.mil/warning/warn-dl.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

(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, therules 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) 283-7755, e-mail peggy.a.irving@m1.irs.gov (note: the number 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.