United States General Accounting Office

GAO

Report to the Chairman
Committee on Governmental Affairs
U.S. Senate

April 2001

INTERNET PRIVACY

Implementation of Federal Guidance for Agency Use of "Cookies"

GAO
Accountability * Integrity * Reliability

GAO-01-424

Contents

Abbreviations

CIO	Chief Information Officer
OIRA	Office of Information and Regulatory Affairs
OMB	Office of Management and Budget

United States General Accounting Office
Washington, DC 20548

April 27, 2001

The Honorable Fred Thompson
Chairman, Committee on Governmental Affairs
United States Senate

Dear Mr. Chairman:

Federal agencies are using Internet "cookies" to enable electronic transactions and track visitors on their Web sites. Cookies are text files that have unique identifiers associated with them and are used to store and retrieve information that allow Web sites to recognize returning users, track on-line purchases, or maintain and serve customized Web pages. Cookies may be classified as either "session" or "persistent." Session cookies expire when the user exits the browser, while persistent cookies can remain on the user's computer for a specified length of time.

In June 2000, the Office of Management and Budget (OMB) issued guidance that addresses the use of cookies on federal Web sites. This guidance established a presumption that persistent cookies would not be used on federal Web sites. Further, it provided that persistent cookies could be used only when agencies (1) provide clear and conspicuous notice of their use, (2) have a compelling need to gather the data on-site, (3) have appropriate and publicly disclosed privacy safeguards for handling information derived from cookies, and (4) have personal approval by the head of the agency.

This report responds to your request that we review federal agencies' use of cookies. Specifically, you asked us to determine whether selected federal Web sites' use of cookies was consistent with OMB's guidance, and whether the guidance issued by OMB provides adequate direction to federal agencies operating public Web sites regarding the use of cookies. In October 2000, at your request, we provided interim information on federal agencies' use of cookies, which indicated that seven agencies were using persistent cookies without disclosing such use.[1]

To address our objectives, we reviewed 65 federal Web sites, including (1) sites operated by 33 high-impact agencies, which handle the majority of

[1] *Internet Privacy: Federal Agency Use of Cookies* (GAO-01-147R, Oct. 20, 2000).

the government's contact with the public, and (2) 32 Web sites randomly selected from the General Services Administration's government domain registry database. We reviewed these Web sites between November 2000 and January 2001, to determine whether they used persistent cookies and whether such use was disclosed in the Web site's privacy policy. We then contacted each agency to determine whether the remaining three requirements in the OMB guidance had been met. We also reviewed OMB's guidance on cookies and interviewed officials from OMB's Office of Information and Regulatory Affairs (OIRA). Further, we interviewed the Chairman of the Chief Information Officers (CIO) Council's Subcommittee on Privacy.

We conducted our review from August 2000 through March 2001, in accordance with generally accepted government auditing standards. Appendix I contains additional information on the scope and methodology of our review. Appendix II contains a list of the 65 sites that we reviewed.

Results in Brief

As of January 2001, most of the Web sites we reviewed were following OMB's guidance on the use of cookies. Of the 65 sites we reviewed, 57 did not use persistent cookies on their Web sites. However, of the eight sites that were using persistent cookies, four did not disclose such use in their privacy policies, as required by OMB. The remaining four sites using persistent cookies did provide disclosure but did not meet OMB's other conditions for using cookies. In addition, four other sites—that did not use cookies—did not post privacy policies on their home pages. When we brought these issues to the attention of each of the agencies, all of them took corrective action or stated that they are planning to take such action.

Although OMB's guidance has proved useful in ensuring that federal Web sites address privacy issues, the guidance remains fragmented, with multiple documents addressing various aspects of Web site privacy and cookie issues. In addition, the guidance does not provide clear direction on the disclosure of session cookies. Finally, OMB officials' stated position to exempt session cookies from disclosure in Web site privacy policies may confuse visitors to federal Web sites. We make recommendations to the Director to modify this guidance to ensure that it provides federal agencies with comprehensive and clear direction on the use of automatic collections—including cookies—of information on their Web sites.

We provided a draft of this report for review and comment to the Director, OMB, on March 26, 2001. OMB did not provide comments.

Background

A cookie is a short string of text that is sent from a Web server to a Web browser when the browser accesses a Web page. The information stored in a cookie includes, among other things, the name of the cookie, its unique identification number, its expiration date, and its domain. When a browser requests a page from the server that sent it a cookie, the browser sends a copy of that cookie back to the server. In general, most cookies are placed by the visited Web site. However, some Web sites also allow the placement of a third-party cookie—that is, a cookie placed on a visitor's computer by a domain other than the site being visited.

Cookies—whether placed by the visited Web site or a third-party—may be further classified as either session cookies or persistent cookies. Session cookies are short-lived, are used only during the current on-line session, and expire when the user exits the browser. For example, session cookies could be used to support an interactive opinion survey. Persistent cookies remain stored on the user's computer until a specified expiration date and can be used by a Web site to track a user's browsing behavior, through potential linkage to other data and whenever the user returns to a site.

Although cookies help enable electronic commerce and other Web applications, persistent cookies also pose privacy risks even if they do not themselves gather personally identifiable information because the data contained in persistent cookies may be linked to persons after the fact, even when that was not the original intent of the operating Web site. For example, links may be established when persons accessing the Web site give out personal information, such as their names or e-mail addresses, which can uniquely identify them to the organization operating the Web site. Once a persistent cookie is linked to personally identifiable information, it is relatively easy to learn visitors' browsing habits and keep track of viewed or downloaded Web pages. This practice raises concerns about the privacy of visitors to federal Web sites.

OMB Has Issued Guidance on Privacy Policies for Federal Web Sites

Concerned about the protection of the privacy of visitors to federal Web sites, OMB directed—in Memorandum 99-18, issued in June 1999—every agency to post clear privacy policies on its principal Web site, other major entry points to agency Web sites, and any Web page where the agency collects substantial personal information from the public. Further, the memorandum stated that such polices must inform Web site visitors what information the agency collects about individuals, why it is collected, and how it is used, and that the policies must be clearly labeled and easily accessed when someone visits the site.

In addition to these specific requirements, the memorandum was accompanied by an attachment entitled “Guidance and Model Language for Federal Web Site Privacy Policies.” OMB attached the guidance and model language for agencies to use, depending on their needs. For example, the discussion in the attachment states that in the course of operating a Web site, certain information may be collected automatically or by cookies, and that in some instances, sites may have the technical ability to collect information and later take additional steps to identify people. The discussion further states that agency privacy policies should make clear whether or not they are collecting this type of information and whether they will take further steps to collect additional information.

In June 2000, OMB issued further guidance specifically concerning the use of cookies on federal Web sites. Memorandum 00-13 had two major objectives. First, it reminded agencies that they are required by law and policy to establish clear privacy policies for their Web activities and to comply with those policies. To this end, the memorandum reiterated the requirement of Memorandum 99-18 for agencies to post privacy policies on their principal Web sites, major entry points, and other Web pages where substantial amounts of personal information are posted. Second, Memorandum 00-13 established a new federal policy regarding cookies by stating that “particular privacy concerns may be raised when uses of Web technology can track the activities of users over time and across Web sites.” This guidance established a presumption that cookies would not be used on federal Web sites. Further, it provided that cookies could be used only when agencies (1) provide clear and conspicuous notice of their use, (2) have a compelling need to gather the data on the Web site, (3) have appropriate and publicly disclosed privacy safeguards for handling information derived from cookies, and (4) have personal approval by the head of the agency. The memorandum also directed agencies to provide a description of their privacy practices and the steps they have taken to ensure compliance with this memorandum as part of their information technology budget submission package.

Concerned about the impact of Memorandum 00-13 on federal Web sites, the Chairman of the CIO Council’s Subcommittee on Privacy subsequently sent a letter to the Administrator of OMB’s OIRA recommending that session cookies be exempt from the requirements of the memorandum. The Chairman noted that the term “cookie” covers a number of techniques used to track information about Web site use, and that there is an important distinction between session and persistent cookies. Although supporting the application of the new policy to persistent cookies, the Chairman recommended that session cookies, which are discarded on completion of a session or expire within a short time frame and are not used to track personal information, not be subject to the requirements of the memorandum. He added that the use of these cookies should, however, continue to be disclosed in the Web sites' privacy statements.

In a September 2000 letter responding to the Chairman, the Administrator agreed that persistent cookies are a principal example of a technique for tracking the activities of users over time and across different Web sites, and, thus, agencies should not use persistent cookies unless they have met the four conditions provided in the guidance. Further, the Administrator noted that Web sites could gather information from visitors in ways that do not raise privacy concerns, such as retaining the information only during the session or for the purpose of completing a particular on-line transaction, without the capacity to track the user over time and across different Web sites. The letter concluded that such activities would not fall within the scope of the new policy.

Most Federal Web Sites Reviewed Followed OMB Cookie Guidance

As of January 2001, most federal Web sites we reviewed followed OMB's guidance on the use of cookies. Of the 65 federal Web sites reviewed, 57 did not use persistent cookies. However, of the eight Web sites using persistent cookies, four did so without disclosing this in their privacy policies, as required by OMB. Two of these four were allowing commercial, third-party sites to place these cookies on the computers of individuals visiting the sites. The four remaining sites using persistent cookies disclosed this use but did not meet OMB's other conditions. In addition, four sites that did not use persistent cookies did not post privacy policies on their home pages.

After we brought these findings to their attention, all 12 agencies either took corrective action or stated that they planned to take such action, as follows:

- The four sites using persistent cookies without disclosing such use have removed those cookies from their Web sites.
- Two of the four sites using persistent cookies with disclosure have now removed them. Regarding the other two sites, one has recently met all of OMB's conditions in order to use persistent cookies. Agency officials responsible for the remaining site have revised their privacy policy to disclose the use of persistent cookies and have stated that they are in the process of seeking approval from the head of the agency to use such cookies.

- All four sites lacking privacy policy notices have now installed such statement hyperlinks on their respective home pages.

OMB's Cookie Guidance Helpful but Fragmented and Unclear

Although OMB's guidance has proved useful in ensuring that federal Web sites address privacy issues, the guidance is fragmented, with multiple documents addressing various aspects of Web site privacy and cookie issues. Guidance concerning cookies is currently contained in two official policy memorandums. These documents, taken together, prompted the CIO Council to recommend clarification of OMB's cookie policy. Although OMB's response provided useful clarification on the requirements for using persistent cookies, OMB has not yet revised the guidance memorandums themselves. Further, the letter to the CIO Council does not appear on OMB's Web site with the two guidance memorandums. As a result, federal agencies may not have ready access to the clarifying letter and may be confused as to requirements on the use of cookies.

OMB's guidance documents also do not provide clear direction on the disclosure requirements for session cookies. Memorandum 99-18 stated that agency privacy policies should make clear whether information is collected automatically through cookies or other techniques, but it did not distinguish between session and persistent cookies. Memorandum 00-13 established the four conditions for cookie use but, again, did not clearly distinguish between session and persistent cookies. This prompted the CIO Council's letter recommending clarification. OIRA's letter in response clarified that Memorandum 00-13 applied only to persistent cookies but did not directly respond to the Council's recommendation that session cookies continue to be disclosed in Web site privacy policies. This left unresolved questions as to what extent the notice requirements from Memorandum 99-18 apply to session cookies.

When we asked OMB to clarify the disclosure requirements for session cookies, OIRA officials stated that session cookies do not present a privacy issue; therefore, no disclosure is required. This position, however, may confuse and mislead federal Web site visitors. For example, under this policy, a federal Web site may state in its privacy policy that it is not using cookies, while it continues to give session cookies. If a site visitor has enabled a browser to detect the presence of cookies, it may not be apparent to the visitor whether the cookies they see are session or persistent. This could raise questions about the practices of the Web site that would not be resolved by viewing the privacy policy.

The Chair of the CIO Council's Subcommittee on Privacy agreed that the issue is one of clarity rather than privacy. Further, he stated that it is better for agencies to choose full disclosure rather than partial, and that it constitutes good customer service to provide such disclosure.

Conclusions

Most federal Web sites we reviewed were following OMB's guidance on the use of cookies. The sites that were not following the guidance either have taken or plan to take corrective action.

The OMB guidance, while helpful, leaves agencies to implement fragmented directives contained in multiple documents. In addition, the guidance itself is not clear on the disclosure requirements for techniques that do not track users over time and across Web sites, such as session cookies. Further, OMB's stated position on the disclosure requirements for session cookies could lead to confusion on the part of visitors to federal Web sites.

Recommendations for Executive Action

To clarify agency requirements on the use of automatic collections of information, including the use of cookies on their Web sites, we recommend that the Director, OMB, in consultation with other parties, such as agency officials and the CIO Council,

- unify OMB's guidance on Web site privacy policies and the use of cookies,
- clarify the resulting guidance to provide comprehensive direction on the use of cookies by federal agencies on their Web sites, and
- consider directing federal agencies to disclose the use of session cookies in their Web site privacy notices.

Agency Comments

We provided a draft of this report for review and comment to the Director, OMB, on March 26, 2001. OMB did not provide comments.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution of it until 30 days from the date of this letter. At that time we will provide copies of the report to Senator Joseph Lieberman, Ranking Member, Senate Committee on Governmental Affairs; Representative Dan Burton, Chairman, and Representative Henry A. Waxman, Ranking Minority Member, House Committee on Government Reform; the Honorable Mitchell E. Daniels, Jr., Director, Office of Management and Budget; and other interested parties. Copies will also be available on GAO's Web site at www.gao.gov.

If you have any questions, please contact me at (202) 512-6240 or Mike Dolak, Assistant Director, at (202) 512-6362. We can also be reached by e-mail at koontzl@gao.gov and dolakm@gao.gov, respectively. Key contributors to this report were Scott A. Binder, Michael P. Fruitman, and David F. Plocher.

Sincerely yours,

Linda D Koontz

Linda D. Koontz
Director, Information Management Issues

Appendix I: Scope and Methodology

To determine the use of cookies by federal agencies, we reviewed 65 federal Web sites—the same sites we reviewed in our October 2000 report.[1] These Web sites consisted of (1) the sites operated by the 33 high-impact agencies, which handle the majority of the government's contact with the public, and (2) 32 sites randomly selected from the General Services Administration's government domain registry database. We reviewed each Web site between November and December, 2000, to determine which were using cookies and the type of cookies given. We also determined whether the sites using persistent cookies (1) provided clear and conspicuous notice of their use, (2) had a compelling need to gather the data on the site, (3) had appropriate and publicly disclosed privacy safeguards for handling information derived from cookies, and (4) had personal approval by the head of the agency. We updated our findings on January 24, 2001.

We performed our review by using Microsoft's Internet Explorer browser, version 5.5. We changed the security settings in the browser to alert us if we were about to receive a cookie. Before we would visit a Web site, we would clear out our computer's cache, cookies, and temporary files and clear our history folder. We then typed in the Universal Resource Locator of the site we were visiting and spent about 10 to15 minutes per site searching through its links to determine if it was using cookies. To document our review, we made a printout of the site's home page and privacy policies. If we found a persistent cookie on the site, we would make a printout of the cookie. After we captured and printed the cookie, we would stop searching and move on to another site.

We contacted the agencies operating the Web sites that were using persistent cookies, notified them of our findings, and asked them to provide written responses detailing actions they planned to take in response to our findings and provide documentation to support their compliance with the Office of Management and Budget's (OMB) guidelines. Specifically, we asked them to support how they (1) provided clear and conspicuous notice that they were using persistent cookies, (2) had a compelling need to gather the data on the site, (3) had appropriate and publicly disclosed privacy safeguards for handling the information derived from cookies, and (4) had obtained the personal approval by the head of the agency. We also contacted the four agencies that did not have privacy policies posted on their home pages, notified them of our findings,

[1] *Internet Privacy: Federal Agency Use of Cookies* (GAO-01-147R, Oct. 20, 2000).

and asked them to provide written responses detailing the actions they planned to take to ensure that their Web sites complied with OMB guidance.

To determine whether the guidance issued by OMB provided adequate direction to federal agencies operating public Web sites, we analyzed the guidance and discussed its intent with representatives of OMB’s Office of Information and Regulatory Affairs. We also met with the Chairman of the Chief Information Officers Council, Subcommittee on Privacy, to obtain the council’s views on additional privacy issues and concerns that needed to be addressed in OMB guidance.

We conducted our review from August 2000 through March 2001, in accordance with generally accepted government auditing standards.

Appendix II: Federal Web Sites Reviewed

Department/Agency	Web site address	Group[a]
Department of Agriculture		
Animal and Plant Health Inspection Service	www.aphis.usda.gov	High-impact agency
Food Safety and Inspection Service	www.fsis.usda.gov	High-impact agency
Food, Nutrition, and Consumer Service	www.fns.usda.gov	High-impact agency
National Agricultural Library	www.nalusda.gov	Random sample
National Genetic Resources Program	www.ars-grin.gov	Random sample
U.S. Department of Agriculture, Forest Service	www.fs.fed.us	High-impact agency
Department of Commerce		
FedWorld	www.fedworld.gov	Random sample
National Weather Service	www.nws.noaa.gov	High-impact agency
The Official U.S. Time	www.time.gov	Random sample
U.S. Census Bureau	www.census.gov	High-impact agency
U.S. Commercial Service	www.usatrade.gov	High-impact agency
U.S. Patent and Trademark Office	www.uspto.gov	High-impact agency
Department of Defense		
ACQWeb	www.acq.osd.mil	High-impact agency
Department of Education		
Office of Student Financial Assistance Programs	www.ed.gov/offices/OSFAP	High-impact agency
Department of Energy		
Albuquerque Operations Office	www.doeal.gov	Random sample
Ames Laboratory	www.ameslab.gov	Random sample
Fernald Environmental Management Project	www.fernald.gov	Random sample
Southeastern Power Administration	www.sepa.fed.us	Random sample
Department of Health and Human Services		
Administration for Children and Families	www.acf.dhhs.gov	High-impact agency
Health Care Financing Administration	www.hcfa.gov	High-impact agency
IGnet	www.ignet.gov	Random sample
National Institute of Allergy and Infectious Diseases	www.hsroad.gov	Random sample
National Institute on Drug Abuse	www.drugabuse.gov	Random sample
U.S. Food and Drug Administration	www.fda.gov	High-impact agency
Department of Housing and Urban Development		
Code Talk[b]	www.codetalk.gov	Random sample
Department of the Interior		
Bureau of Land Management	www.blm.gov	High-impact agency
National Park Service	www.nps.gov	High-impact agency
Department of Justice		
Federal Bureau of Investigation	www.fbi.gov	Random sample
Immigration & Naturalization Service	www.ins.usdoj.gov	High-impact agency
Department of Labor		
Bureau of Labor Statistics	www.bls.gov	Random sample
Occupational Safety & Health Administration	www.osha.gov	High-impact agency
Department of State		
Bureau of Consular Affairs	www.travel.state.gov	High-impact agency
International Information Programs	www.usia.gov	Random sample

Department/Agency	Web site address	Group[a]
Department of Transportation		
Central Federal Lands Highway Division	www.cflhd.gov	Random sample
Federal Aviation Administration	www.faa.gov	High-impact agency
Department of the Treasury		
Customs Service	www.customs.gov	High-impact agency
Financial Management Service	www.fms.treas.gov	High-impact agency
Internal Revenue Service	www.irs.ustreas.gov	High-impact agency
Department of Veterans Affairs	.	
Veterans Benefits Administration	www.vba.va.gov	High-impact agency
Veterans Health Administration	www.va.gov/About_VA/Orgs/VHA/index.htm	High-impact agency
Independent agencies		
African Development Foundation	www.adf.gov	Random sample
Environmental Protection Agency	www.epa.gov	High-impact agency
Farm Credit Administration	www.fca.gov	Random sample
Farm Credit System Insurance Corporation	www.fcsic.gov	Random sample
Federal Communications Commission	www.fcc.gov	Random sample
Federal Emergency Management Agency	www.fema.gov	High-impact agency
Federal Retirement Thrift Investment Board	www.frtib.gov	Random sample
Federal Trade Commission	www.ftc.gov	Special selection
FinanceNet	www.financenet.gov	Random sample
General Services Administration	www.gsa.gov	High-impact agency
Institute of Museum and Library Services	www.imls.fed.us	Random sample
National Aeronautics and Space Administration	www.nasa.gov	High-impact agency
National Credit Union Administration	www.ncua.gov	Random sample
National Science Foundation, Directorate for Computer and Information Science and Engineering	www.cise.nsf.gov	Random sample
Occupational Safety and Health Review Commission	www.oshrc.gov	Random sample
Office of the Federal Environmental Executive	www.ofee.gov	Random sample
Office of Personnel Management	www.opm.gov	High-impact agency
Small Business Administration	www.sba.gov	High-impact agency
Social Security Administration	www.ssa.gov	High-impact agency
The Access Board	www.access-board.gov	Random sample
The White House Fellows Program	www.whitehousefellows.gov	Random sample
Thrift Savings Plan	www.tsp.gov	Random sample
U.S. Nuclear Regulatory Commission	www.nrc.gov	Random sample
U.S. Postal Service	new.usps.com	High-impact agency
U.S. Trade and Development Agency	www.tda.gov	Random sample

[a]High-impact agencies handle the majority of the government's contact with the public. The random sample Web sites were selected from the General Services Administration's government domain registry database. The special selection was the Federal Trade Commission's Web site.

[b]Code Talk is a Web site that is hosted but not owned by HUD.

(310308)

Ordering Information

The first copy of each GAO report is free. Additional copies of reports are $2 each. A check or money order should be made out to the Superintendent of Documents. VISA and MasterCard credit cards are also accepted.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:
U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

Orders by visiting:
Room 1100
700 4th St., NW (corner of 4th and G Sts. NW)
Washington, DC 20013

Orders by phone:
(202) 512-6000
fax: (202) 512-6061
TDD (202) 512-2537

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

Orders by Internet
For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to:

Info@www.gao.gov

or visit GAO's World Wide Web home page at:

http://www.gao.gov

To Report Fraud, Waste, and Abuse in Federal Programs

Contact one:

- Web site: http://www.gao.gov/fraudnet/fraudnet.htm
- E-mail: fraudnet@gao.gov
- 1-800-424-5454 (automated answering system)