GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

Accounting and Information
Management Division

B-286150

September 11, 2000

The Honorable Dick Armey
Majority Leader
House Of Representatives

The Honorable W. J. Billy Tauzin
Chairman, Subcommittee on Telecommunications,
Trade and Consumer Protection
Committee on Commerce
House Of Representatives

Subject: Internet Privacy: Comparison of Federal Agency Practices With FTC's Fair Information Principles

On-line privacy has emerged as one of the key—and most contentious—issues surrounding the continued evolution of the Internet. The World Wide Web requires the collection of certain data from individuals who visit web sites—such as Internet address—in order for the site to operate properly. However, collection of even this most basic data can be controversial because of the public's apprehension about what information is collected and how it could be used.

Concerned about the exponential growth of the on-line consumer marketplace and the capacity of the on-line industry to collect, store, and analyze vast amounts of data about consumers visiting commercial web sites, the Federal Trade Commission (FTC) reported in May 2000 on its most recent privacy survey of commercial web sites. The survey's objective was to assess the on-line industry's progress in implementing four fair information principles which FTC believes are widely accepted.

- Notice. Data collectors must disclose their information practices before collecting personal information from consumers.
- Choice. Consumers must be given options with respect to whether and how personal information collected from them may be used for purposes beyond those for which the information was provided.
- Access. Consumers should be able to view and contest the accuracy and completeness of data collected about them.

- Security. Data collectors must take reasonable steps to ensure that information collected from consumers is accurate and secure from unauthorized use.

In addition, the survey looked at the use of third-party cookies[1] by commercial web sites. Although FTC noted improvement over previous surveys, it nonetheless concluded that the on-line industry's self-regulatory initiatives were falling short. As a result, a majority of the FTC commissioners, based on a 3 to 2 vote, recommended legislation to require commercial web sites not already covered by the Children's Online Privacy Protection Act (COPPA)[2] to implement the four fair information principles.

While the FTC's fair information principles address Internet privacy issues in the commercial sector, federal web sites are governed by specific laws designed to protect individuals' privacy when agencies collect personal information. The Privacy Act of 1974 is the primary law regulating the federal collection and maintenance of personal information maintained in a federal agency's systems of records.[3] The act provides, for example, that (1) agencies cannot disclose such records without the consent of the individual except as authorized by law, (2) under certain conditions, individuals can gain access to their own records and request corrections, and (3) agencies must protect records against disclosure and loss. While these requirements are generally consistent with FTC's fair information principles, the act's specific provisions limit the application of these principles to the federal government. Specifically, the Privacy Act applies these principles only to information maintained in a system of records and contains exceptions that allow, under various circumstances, the disclosure and use of information without the consent of the individual. On June 2, 1999, OMB provided additional guidance on Internet privacy issues in Memorandum M-99-18, directing agencies to post privacy policies on principal federal web sites that disclose what information is collected, why it is collected, and how it will be used. In a separate report issued earlier this month,[4] we evaluated selected federal web sites' privacy policies against certain aspects of applicable laws and guidance, and included a comparison of the Fair Information Principles and the Privacy Act. We also have ongoing work—which we intend to report on later this year—addressing in greater depth the use of cookies on federal web sites.

This letter responds to your request that we determine how federal web sites would fare when measured against FTC's fair information principles for commercial web sites. In

[1]A cookie is a small text file placed on a consumer's computer hard drive by a web server. The cookie transmits information back to the server that placed it, and, in general, can be read only by that server. A third-party cookie is placed on a consumer's computer hard drive by a web server other than the one being visited by the consumer--often without the consumer's knowledge. Enclosure IV contains further explanation on cookies.

[2]15 U.S.C. 6501 et seq. The provisions of COPPA govern the collection of information from children under the age of 13 at web sites, or portions of web sites, directed to children or which have actual knowledge that a user from which they seek personal information is a child under 13 years old. These provisions took effect April 21, 2000.

[3]A system of records means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

[4]*Internet Privacy: Agencies' Efforts to Implement OMB's Privacy Policy*, GAO/GGD-00-191, September 2000.

applying FTC's methodology, we analyzed a sample of federal web sites to determine whether they collected personal identifying information, and if so, whether the sites included disclosures to indicate they met the fair information principles of Notice, Choice, Access, and Security. We also determined the extent to which these sites allowed the placement of third-party cookies and disclosed to individuals that they may allow the placement of these cookies. We did not, however, verify whether the web sites follow their stated privacy policies. It should be noted that FTC staff have expressed concern about this use of their methodology, stating that there are fundamental differences between federal and commercial web sites which, in their view, make FTC's methodology inappropriate for use in evaluating federal web site privacy policies. For example, an agency's failure to provide for Access or Choice on its privacy policy may reflect the needs of law enforcement or the dictates of the Privacy Act or other federal statutes that do not apply to sites collecting information for commercial purposes.

As requested by your offices, we used FTC's methodology to provide a snapshot of the privacy practices of two groups of web sites operated by executive branch agencies against the fair information principles. We reviewed a total of 65 sites during July 2000. One group consisted of web sites operated by 32 high-impact agencies, which handle the majority of the government's contact with the public.[5] A second group consisted of web sites randomly selected from the General Services Administration's (GSA) government domain registration database.[6] This group consisted mostly of web sites operated by small agencies, commissions, or programs. Finally, at your request, we assessed the FTC web site itself. (For the purpose of our analysis, the FTC site was added to the sites operated by the 32 high-impact agencies.)

We obtained comments on this report from OMB and several agencies that are summarized at the end of this letter, and we have included OMB's comments in their entirety as enclosure I. A list of the 65 federal web sites we reviewed is included as enclosure II. Enclosure III contains a more detailed discussion of our scope and methodology.

RESULTS IN BRIEF

As of July 2000, all of the 65 web sites in our survey collected personal identifying information[7] from their visitors, and 85 percent of the sites posted a privacy notice. The majority of these federal sites (69 percent) also met FTC's criteria for Notice. However, a much smaller number of sites implemented the three remaining principles—Choice (45 percent), Access (17 percent), and Security (23 percent). Few of the federal sites—3 percent—implemented elements of all four of FTC's fair information principles. Finally, a small number of sites (22 percent) disclosed that they may allow third-party cookies; 14 percent actually allowed their placement.

[5]According to the National Partnership for Reinventing Government, these agencies handle 90 percent of the federal government's contact with the public.

[6]Our random sample was not large enough to project to the universe of federal web sites.

[7]Information used to identify or locate an individual, e.g., name, address, e-mail address, credit card number, Social Security number, etc.

BACKGROUND

FTC is an independent agency created under the Federal Trade Commission Act in 1914 to protect consumers from unfair or deceptive practices in and affecting commerce. According to FTC, the act authorizes it to seek injunctive relief, including redress, for violations, by entities engaged in or whose business affects commerce, including commerce on the Internet.

Federal agencies must comply with a number of laws relating to privacy protection, particularly the Privacy Act of 1974. In addition, the Office of Management and Budget (OMB) has issued implementing guidance to federal agencies.

FTC's Studies of On-line Privacy

FTC's specific authority over the collection and dissemination of personal data collected on-line stems from section 5 of the FTC Act and COPPA, which FTC has the authority to enforce. FTC has brought several cases against online companies who failed to comply with their stated information principles. However, according to the FTC, it generally lacks authority to require firms to adopt information policies on their web sites, or portions of their web sites, not directed toward children.

FTC has been studying on-line privacy since 1995 and has issued three reports to the Congress. FTC issued a report in 1998 summarizing the four fair information practice principles of Notice, Choice, Access, and Security regarding the collection, use, and dissemination of personal information.[8] FTC's 1998 report also presented the results of their first online privacy survey of commercial web sites.

In a 1999 report based in part on a survey conducted by Georgetown University, FTC recommended that industry self-regulation be given more time, yet called for further industry efforts to implement the fair information principles.[9] FTC's May 2000 report is based on a more recent survey of commercial web sites to evaluate their compliance with the fair information principles.[10] The May 2000 report examined web sites with more than 39,000 unique visitors in the month of January 2000, and identified two separate groups: (1) a random sample of all the sites—the random sample, and (2) the 100 busiest sites—the most popular group. The random sample consisted of 335 web sites; the most popular group included 91 of the 100 busiest sites on the web.

While the survey showed a significant increase in the proportion of commercial web sites posting at least one privacy disclosure—from 71 percent in 1998 to 100 percent in 2000 for the most popular group and from 14 percent in 1998 to 88 percent in 2000 for the random sample—FTC concluded that the on-line industry had achieved limited success

[8] *Privacy Online: A Report to Congress,* Federal Trade Commission, June 1998.
[9] *Self-Regulation and Privacy Online: A Report to Congress,* Federal Trade Commission, July 1999.
[10] *Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress,* Federal Trade Commission, May 2000.

in implementing the four fair information principles. It noted that of web sites collecting personal identifying information, 42 percent in the most popular group and 20 percent in the random sample implemented, at least in part, each of the four fair information principles.

FTC reported that, of web sites collecting personal identifying information, 60 percent in the most popular group and 41 percent in the random sample implemented two of the key core principles—Notice and Choice. FTC also found that a portion of the commercial web sites implemented Access and Security—83 percent of the web sites collecting personal identifying information in the most popular group and 43 percent of the sites collecting personal identifying information in the random sample for Access, and 74 percent and 55 percent, respectively, for Security. Finally, FTC reported that 78 percent of the sites in the most popular group and 57 percent of the sites in the random sample allowed third parties to place cookies on consumer's computers. However, only 51 percent of sites in the most popular group that allows third-party cookies and 22 percent of such sites in the random sample posted a disclosure about third-party cookie placement. (See enclosure IV on how cookies are made.)

Based on these survey results and citing ongoing consumer concerns regarding privacy on-line and the limited success of self-regulatory efforts to date, a 3-2 majority of the FTC commissioners proposed that legislation be passed that would require all consumer-oriented commercial web sites that collect personal identifying information from or about consumers online—to the extent not already covered by COPPA—to implement the four fair information principles. The same majority of FTC commissioners also proposed that the legislation provide an implementing agency with authority to set more detailed standards pursuant to the Administrative Procedure Act,[11] including authority to enforce those standards.

Laws and Guidance Governing On-line Privacy
Of Federal Web Sites

While FTC's authority extends to commercial sites, several types of federal guidance cover similar areas for government-run sites. The enactment of the Privacy Act was influenced by Fair Information Practice Principles that were first articulated in July 1973 when a Department of Health, Education and Welfare (HEW) Advisory Committee on Automated Personal Data Systems issued a report entitled, "Records, Computers, and the Rights of Citizens." These principles have evolved over time and were summarized by FTC in the four fair information principles it has proposed as standards for commercial web sites. While the Privacy Act and other federal laws[12] generally contain most of the fair information principles, the laws' specific requirements—regarding access to information collected by federal agencies and an agency's ability to offer a submitter choices about the use of their data—result in differences between how the principles are

[11]5 U.S.C. 553.

[12]Other laws of general application that apply are the Freedom of Information Act which was enacted in 1966, the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, the Computer Matching and Privacy Protection Act of 1988, and the Federal Records Act.

currently applied in the federal government and how FTC envisions their application in the commercial sector.

The Privacy Act places limits on the collection, use, and dissemination of personally identifiable information about an individual maintained by an agency and contained in an agency's system of records; for example, under certain conditions, it grants individuals the right of access to agency records pertaining to themselves, the right to amend a record if inaccurate, irrelevant, untimely, or incomplete, and the right to sue the government for violations of the act. The protection offered by the Privacy Act is augmented by other laws designed to protect an individual's right to privacy when personal information is collected.

In addition to pertinent laws, OMB has provided guidance to agencies. Its Circular No. A-130, appendix I, "Federal Agency Responsibilities for Maintaining Records About Individuals" provides guidance on implementation of the Privacy Act. This guidance establishes policies for the management of federal information resources, as required by the Paperwork Reduction Act, as amended.[13] The circular sets forth a number of general policies concerning the protection of personal privacy by the federal government. For example, agencies have a responsibility to limit the collection of information that identifies individuals to that which is legally authorized and necessary for the proper performance of agency functions. Agencies must also provide individuals, upon request, with access to records about them, and permit them to amend such records consistent with the provisions of the Privacy Act.

On June 2, 1999, OMB issued Memorandum M-99-18, directing agencies to post privacy policies on federal web sites that disclose what information is collected, why it is collected, and how it will be used. On June 22, 2000, OMB issued Memorandum M-00-13, providing additional guidance on the limited circumstances under which federal web sites may collect information through the use of cookies.

FEDERAL WEB SITES SURVEYED COLLECT PERSONAL DATA BUT VARY IN DEGREE OF CONFORMITY TO FTC PRINCIPLES

We found that all of the 65 web sites surveyed collected personal identifying information from their visitors. Most sites—85 percent—posted a privacy notice. However, they varied in the extent to which they provided Notice to consumers, allowed consumers Choice and Access regarding their information, disclosed that they provided Security for the information provided, and allowed and disclosed the placement of third-party cookies.

Using the same scoring methodology that FTC used for commercial sites, our survey showed that only 6 percent of the federal high-impact agencies and 3 percent of the randomly sampled sites federal web sites implemented, at least in part, each of the four fair information principles. The following figures depict how the federal web sites in our

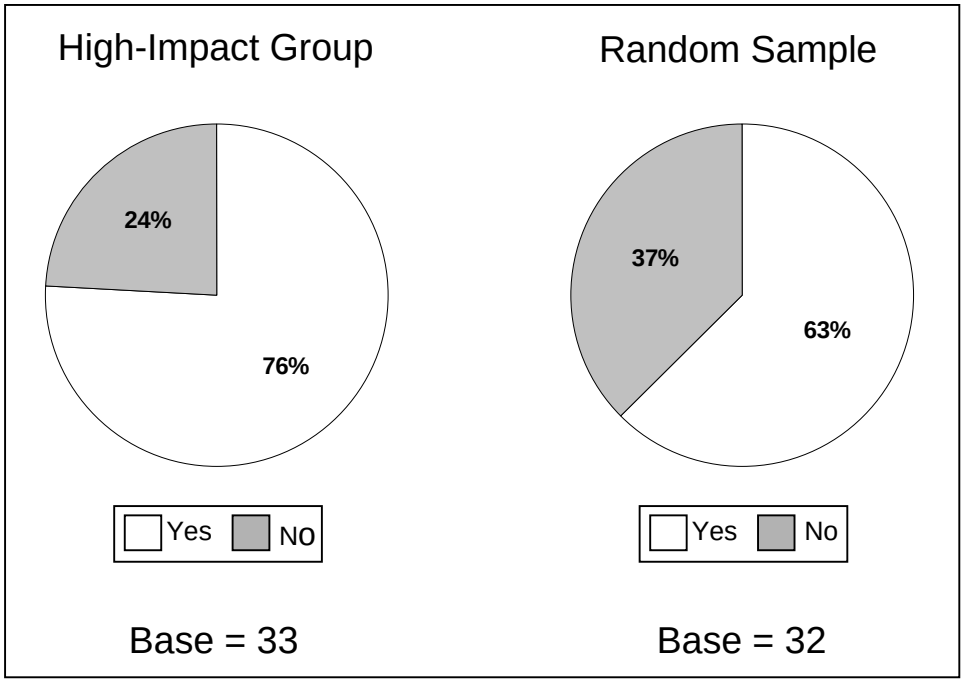
[13] P.L. 96-511, 99-500 and 99-591, and 104-13.

survey fared in conforming with each of the principles. For each figure, an explanation is provided of how we scored the sites to determine conformance with the principle.

Notice

The Notice principle is a prerequisite to implementing the other principles. We concluded that a site provided Notice if it met all of the following criteria: (1) posted a privacy policy, (2) stated anything about what specific personal information it collects, (3) stated anything about how the site may use personal information internally, and (4) stated anything about whether it discloses personal information to third parties. Our survey showed that 69 percent of all sites visited met FTC's criteria for Notice. Figure 1 shows the percentages of sites implementing Notice for each group.

Figure 1: Percentage of Sites Collecting Personal Identifying Information That Implemented Notice

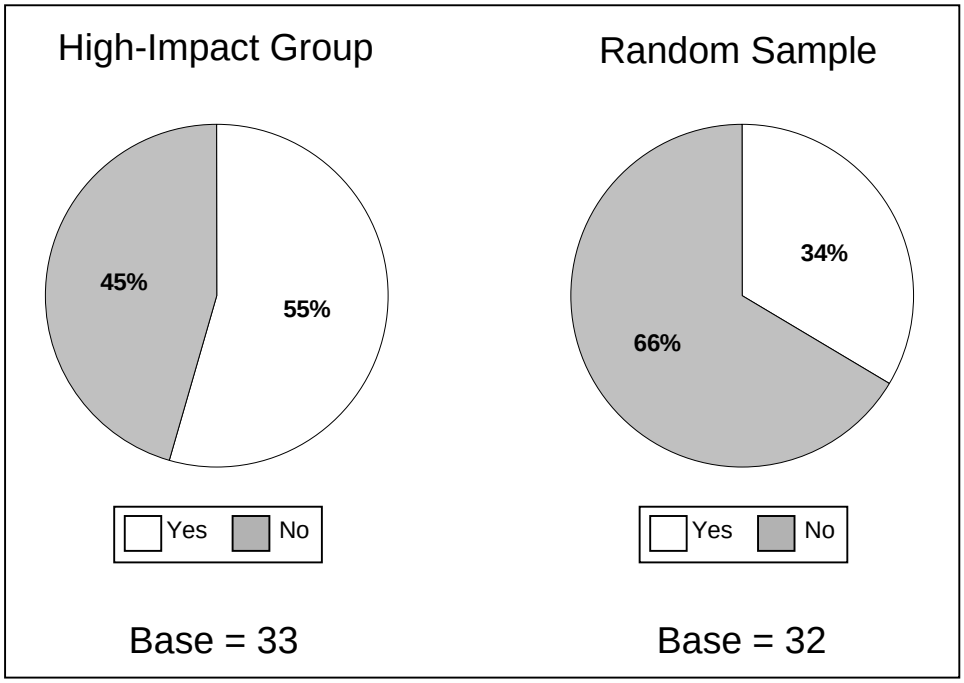


Choice

Under the Choice principle, web sites collecting personal identifying information must afford consumers an opportunity to consent to secondary uses of their personal information, such as the placement of consumers' names on a list for marketing additional products or the transfer of personal information to entities other than the data collector. Consistent with such consumer concerns, FTC's survey included questions about whether sites provided choice with respect to their internal use of personal information to send communications back to consumers (other than those related to processing an order) and whether they provided choice with respect to their disclosure of personal identifying information to other entities, defined as third-party choice.

We concluded that a site provided Choice if both internal choice with respect to at least one type of communication with the consumer and third-party choice with respect to at least one type of information were given to individuals. Our survey showed that 45 percent of all sites met FTC's criteria for Choice. Figure 2 shows the percentages of sites implementing Choice for each group.

Figure 2: Percentage of Sites Collecting Personal Identifying Information That Implemented Choice

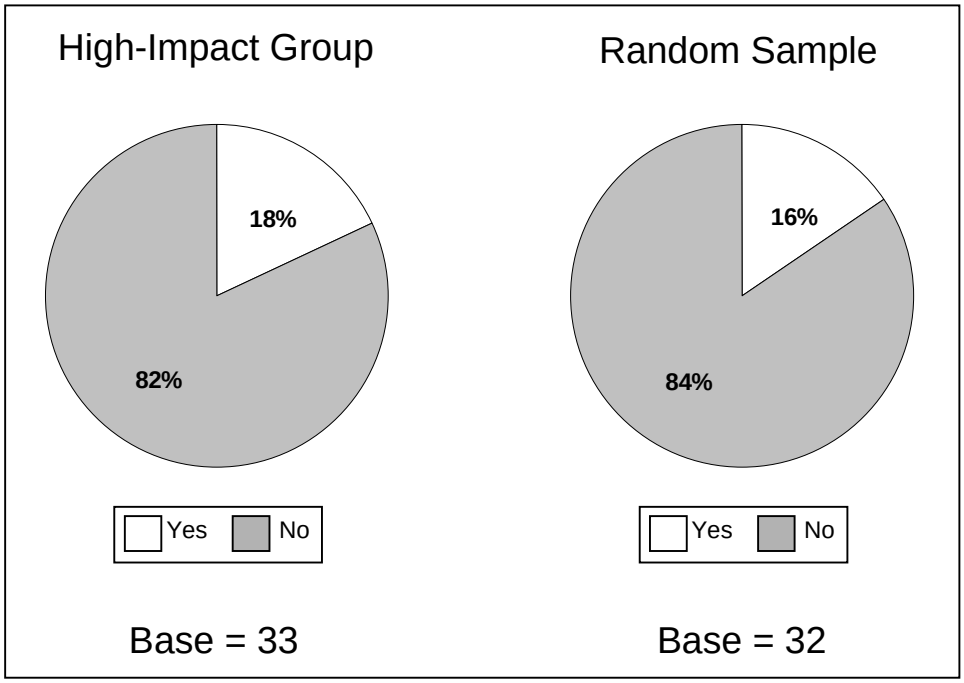


Access

Access refers to an individual's ability both to access data about himself or herself—to view the data in the web site's files—and to contest that data's accuracy and completeness. Access is essential to improving the accuracy of data collected, which benefits both data collectors who rely on such data and consumers who might otherwise be harmed by adverse decisions based on incorrect data. FTC's survey asked three questions about Access: whether the site stated that it allows consumers to (1) review at least some personal information about them, (2) have inaccuracies in at least some personal information about themselves corrected, and (3) have at least some personal information deleted.

We concluded that a site provided Access if it provided any one of these disclosures. Our survey showed that 17 percent of all sites met the FTC criteria for Access. Figure 3 shows the percentages of sites implementing Access for each group.

Figure 3: Percentage of Sites Collecting Personal Identifying Information That Implemented Access

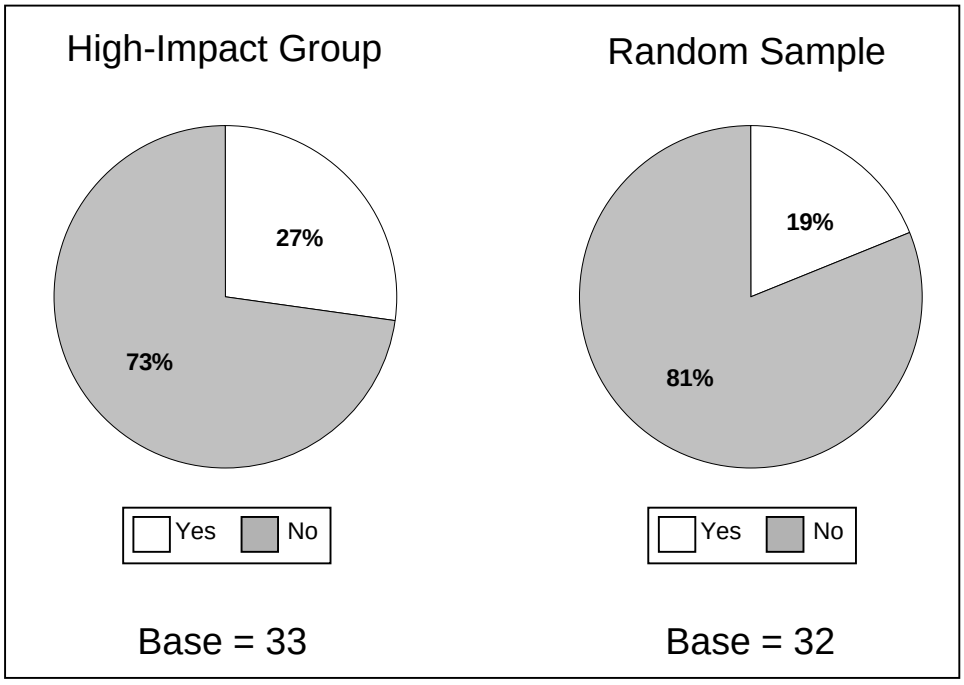


Security

Security refers to the protection of personal information against unauthorized access, use, or disclosure, and against loss or destruction. Security involves both management and technical measures to provide such protections. FTC's survey asked whether sites disclose that they (1) take any steps to provide security, and if so, whether they (2) take any steps to provide security for information during transmission, or (3) take any steps to provide security for information after receipt.

We concluded that a site provided Security if it made any disclosure regarding security. Our survey showed that 23 percent of all sites met FTC's criteria for Security. Figure 4 shows the percentages of sites implementing Security for each group.

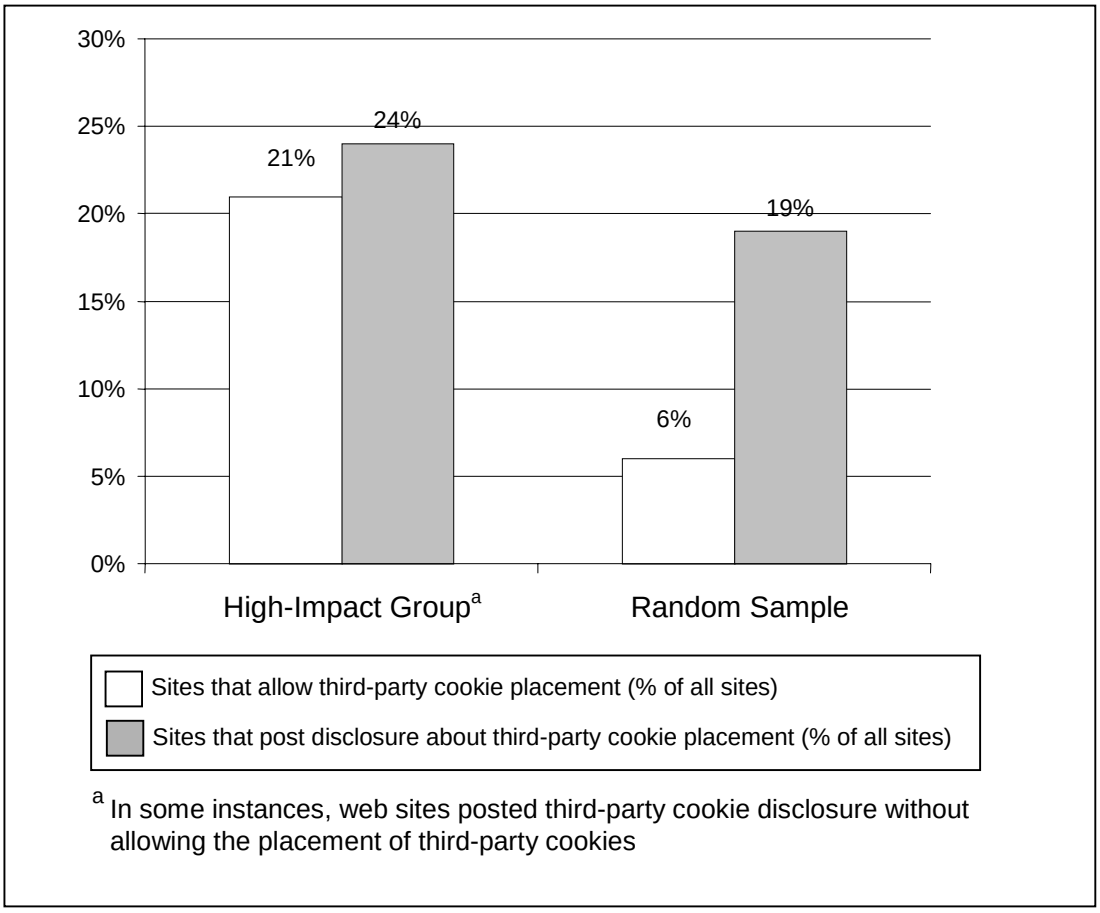
Figure 4: Percentage of Sites Collecting Personal Identifying Information That Implemented Security



Third-Party Cookies

FTC defines a third-party cookie as a cookie placed on a consumer's computer by any domain other than the site being surveyed. Typically, in the commercial environment, the third party is an on-line marketing organization, or an on-line service that tracks and tabulates web-site traffic. However, some federal web sites also allow placement of third-party cookies. Our survey showed that 22 percent of all sites disclosed that they may allow third-party cookies and 14 percent allowed their placement. Figure 5 illustrates the percentages of sites that disclose potential placement of third-party cookies and allow their placement in each group.

Figure 5: Third-Party Cookies: Placement and Disclosure Rates



AGENCY COMMENTS AND OUR EVALUATION

On August 25, 2000, we requested comments on a draft of this letter from OMB and the agencies from our survey that—in response to a previous inquiry—had indicated a desire to provide comments. In a letter dated September 7, 2000, OMB's Deputy Director for Management said that federal agencies have made significant progress in protecting personal privacy on-line and OMB is committed to continuing this improvement. The

Deputy Director said, however, that she believes our summary statistics are misleading because (1) FTC's fair information principles are designed for commercial web sites where the Privacy Act does not apply, and (2) federal agencies have been directed to follow the Privacy Act and OMB guidance, not FTC's fair information principles. (See enclosure I for a copy of OMB's letter.) The Environmental Protection Agency (EPA), the Internal Revenue Service (IRS), and the Department of the Treasury expressed similar concerns. Our report discloses the current requirements governing federal web sites and FTC's concern that its methodology was developed for commercial web sites, not federal web sites.

The Department of Education commented that its Office of Student Financial Assistance Programs (OSFAP) web site—which was part of our sample—does not collect personal information even though we say that all 65 web sites in our survey do. The web sites we reviewed are included as enclosure II. During our survey we found that the OSFAP site did collect personal identifying information, for example, an e-mail address on a customer feedback form.

Treasury commented that the report does not distinguish between sites that collect and retain personal information and sites that only respond to queries through e-mail. Similarly, EPA stated that most agencies give notice that they will not use information collected on their sites except for clearly defined purposes such as collecting a user's e-mail address in order to respond to them. EPA further stated that in this case, agencies should not be expected to post notices about the other principles since there is a clear choice open to the user. According to FTC's methodology and definition, a user providing an e-mail address constitutes collection of personal identifying information. We applied this same methodology to the federal sites.

We also received technical comments from FTC and the Department of Housing and Urban Development which we have incorporated as appropriate into the report. In addition, the Department of Veterans Affairs, the Federal Communications Commission, and IRS provided information on their current or planned actions with regard to citizens' on-line privacy.

- - - - -

We conducted our review in July and August 2000, in accordance with generally accepted government auditing standards. As agreed with your offices, unless you publicly announce the contents of the report earlier, we will not distribute it until 30 days from the date of this letter. At that time, we will send copies to the Honorable Jacob J. Lew, Director, Office of Management and Budget. We will also send copies to Senators John McCain, Chairman, and Ernest Hollings, Ranking Minority Member, Senate Committee on Commerce, Science, and Transportation; Senators Fred Thompson, Chairman, and Joseph Lieberman, Ranking Minority Member, Senate Committee on Governmental Affairs; Representatives Tom Bliley, Chairman, and John D. Dingell, Ranking Minority Member, House Committee on Commerce; and Representatives Dan Burton, Chairman, and Henry A. Waxman, Ranking Minority Member, House Committee on Government Reform. Copies will also be made available to others upon request.

Please contact me at (202) 512-6240 if you or your staff have any questions. I can also be reached by e-mail at *koontzl.aimd@gao.gov*. Key contributors to this letter were Ronald B. Bageant, Scott A. Binder, Mirko J. Dolak, Michael P. Fruitman, Pamlutricia Greenleaf, William N. Isrin, Michael W. Jarvis, Kenneth A. Johnson, Glenn R. Nichols, David F. Plocher, Jamie M. Pressman, and Warren Smith.

Linda D. Koontz
Associate Director, Governmentwide and Defense
Information Systems

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

DEPUTY DIRECTOR
FOR MANAGEMENT

September 7, 2000

Linda D. Koontz
Associate Director, Government-Wide
and Defense Information Systems
General Accounting Office
Washington, DC 20548

Dear Ms. Koontz:

Thank you for the opportunity to comment on GAO's draft report, "Internet Privacy: Comparison of Federal Agency Practices with FTC's Fair Information Principles."

This report addresses a subject that is very important to this Administration - the protection of personal privacy online. Federal agencies have made significant progress in this area, and we believe that the summary statistics in the report, are seriously misleading for two principal reasons. First, the fair information practices that apply to Federal systems of records are set forth by law in the Privacy Act of 1974, whereas the precise language of the FTC's fair information practices was designed for commercial websites where the Privacy Act does not apply. Second, because of this legal difference, agencies have been directed to follow the Privacy Act and OMB policy on website privacy policies rather than the FTC formulation of fair information practices.

Last spring OMB Director Jack Lew issued Memorandum M99-18, "Privacy Policies on Federal Websites," in response to questions and concerns raised by the public about federal agency use of personal information collected online. In that memorandum, OMB directed federal agencies to post privacy policies on key web pages on agency websites. The executive branch agencies implemented the OMB memorandum with great success. As shown in a separate GAO report on "Internet Privacy: Agencies' Efforts to Implement OMB's Privacy Policies," agencies have now adopted privacy policies at the most important web pages on their sites, with a virtually perfect record at agency principal websites and at major points of entry. When GAO conducted its review of the principal websites at 70 agencies, 69 of them had a privacy policy posted. In addition, GAO identified 2,692 major points of entry on six agencies' websites -- all but 9 had privacy policies posted. This success is all the more impressive because it occurred when agencies were also occupied with intensive Y2K preparations.

Not only are the FTC's fair information practices different from the policy set for Federal agencies, but it is odd as well as misleading to measure Federal agency compliance with standards designed for commercial sites. For instance, a central privacy issue on commercial websites is whether individuals have a choice before their personal information is shared with other companies. Commercial websites vary widely on their policies on this issue, and it is crucial for commercial sites to inform consumers of their practices. Sites may be held accountable under the Federal Trade Commission Act for deceptive practices only when they have made a promise in their privacy policy and then failed to follow

that promise. By contrast, the Privacy Act provides as a matter of law that information in a system of records can only be shared with consent of the individual or under other applicable law. Furthermore, OMB policy under Circular A-130 is that federal agencies may not sell personal information for a profit. Thus, in the commercial sector the "choice" principle must be stated in the privacy policy for legal protections to apply, whereas in Federal agencies the information is protected as a matter of law and governmentwide policy.

Similar differences exist with respect to the access and security principles. For access, commercial sites are held accountable under law based on the terms of their privacy policy. By contrast, the Privacy Act guarantees individuals the right to access information about them held in Federal systems of records. Similarly, commercial sites bind themselves legally to certain security practices based on what they say in their privacy policies. But Federal agencies are required to provide good security under the Clinger-Cohen Act, the Computer Security Act, and numerous other laws and policies. The measure of good security is good security, not whether a Federal website makes a brief statement saying that security is protected.

The longstanding practice in the United States has been to tailor privacy laws and policies to the needs of the particular sector. Since the 1970s, we have had specific requirements for fair information practices for credit reports and for Federal systems of records. More recently, we have developed specific rules for especially sensitive information in financial and medical records and for websites targeted at children. Because the laws differ for these various sectors, and because the sensitivity of the data and the intended uses of data also differ, great caution is needed in applying the standards from one sector, such as commercial websites, to another sector, such as Federal agency websites.

In conclusion, we are concerned that the summary statistics in this report are comparable to a complaint that an apple lacks a thick, orange rind. We are committed to continuing to improve the privacy policies and practices of Federal agency websites. But we think that little is gained by measuring the quality of those websites with criteria that differ from the policy set for agencies and that were designed for other purposes.

Sincerely,

Sally Katzen
Deputy Director for Management

-2-

ENCLOSURE II ENCLOSURE II

LIST OF FEDERAL WEB SITES REVIEWED

Agency/Department	Web Site Address	Group
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
USDA 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[14]	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

[14] Code Talk is an interagency site that is hosted but not owned by HUD.

Department of State		
Bureau of Consular Affairs	www.travel.state.gov	High-Impact Agency
International Information Programs	www.usia.gov	Random Sample
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 CISE	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

ENCLOSURE III ENCLOSURE III

SCOPE AND METHODOLOGY

In conducting our survey we generally followed the FTC methodology, including the selection of similar groups of web sites and the use of its data-collection forms and analytical techniques. According to FTC's deputy general counsel, however, because commercial and government web sites are fundamentally different, FTC believes that the survey that it used for commercial web sites is not well suited for assessing the privacy of government web sites. He further said that federal web sites are not in the business of selling or marketing individuals' information, and are governed by different laws concerning individuals' access to information and individuals' choices regarding how their data is used, shared, transferred, or disposed of.

Sample Selection

The FTC survey was based on two target populations drawn from a list of the busiest commercial web sites in the month of January 2000: the 100 most popular U.S. commercial sites and a random sample of all web sites with at least 39,000 unique visitors. Both were drawn from data provided by a commercial web rating service. Because federal web sites are not rated for popularity or frequency of access, we relied on other measures to select our two sample groups.

To survey a group similar to the FTC most popular group, we selected the web sites of 32 high-impact federal agencies that, according to the National Partnership for Reinventing Government, handle 90 percent of the federal government's contact with the public. To survey a group similar to FTC's random sample, we randomly selected 32 active web sites operated by executive branch agencies from the GSA's government domain registration database.[15] Because of time limitations, we were unable to select a random sample large enough to allow us to statistically project our findings to the universe of executive branch agencies' web sites. At your request, we included the FTC web site in our survey and for analysis purposes added it to the high-impact agencies.

Training

We requested—and received—training from FTC similar to that provided to staff who collected and analyzed its survey information. Our staff underwent 2 half-days of training by FTC staff on its methodology and content analysis procedures for commercial web sites.

Information Collection

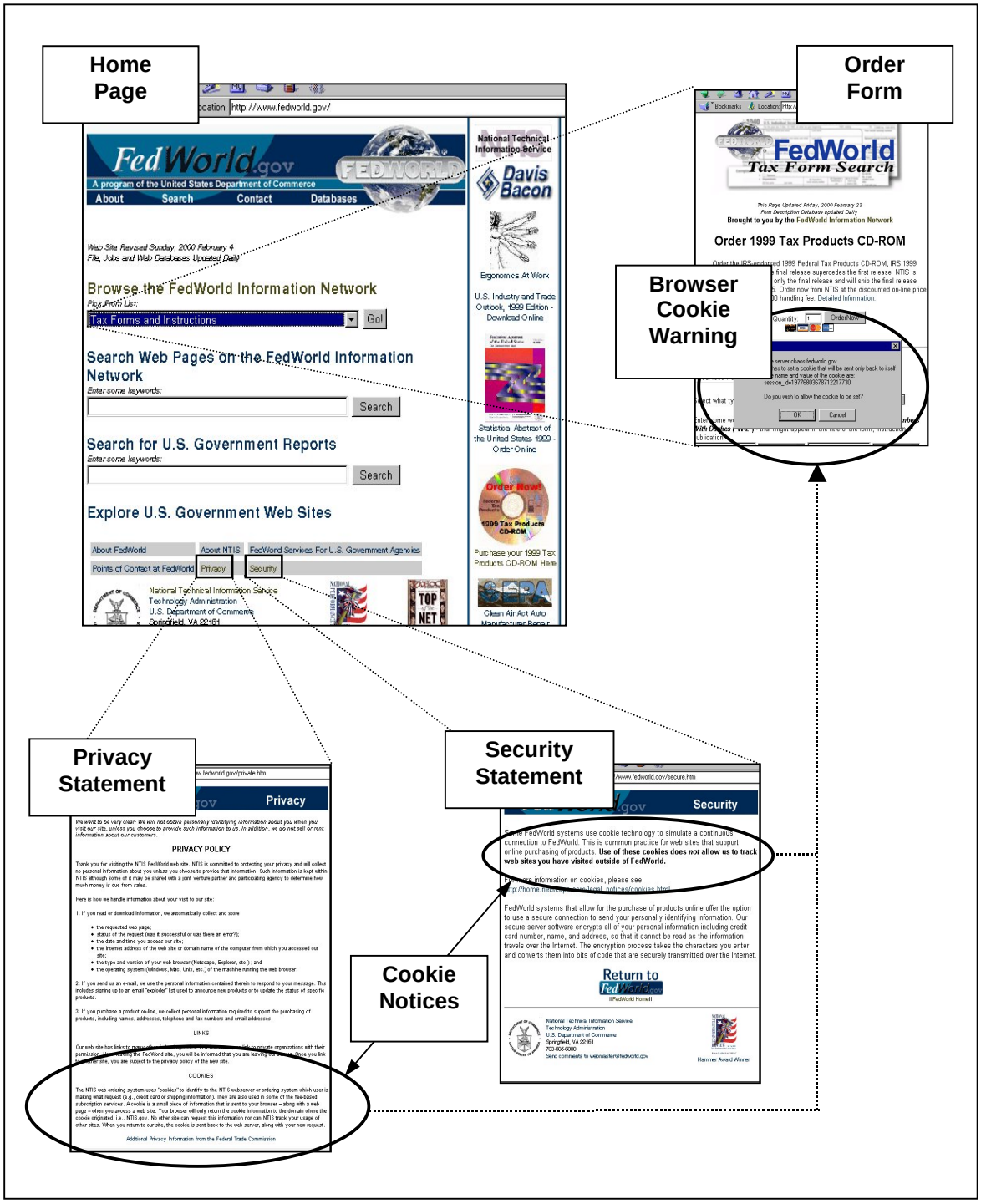
We visited the web sites in our samples from July 12 through July 21, 2000. We reviewed the web pages within the site—for up to a time limit of 15 minutes—to determine whether the site collected any personal or personal identifying information, posted a privacy statement, information practice statement, or disclosure notice, provided

[15]GSA serves as the registrar for the federal .gov domains.

individual access to and choice regarding use of the information, and provided security over the information. We also looked for the placement and disclosure of third-party cookies.

Federal web sites in our samples varied greatly as to their appearance, how much personal identifying information they collected, and their notification to the user of the placement of cookies. Figure 6 shows a typical federal web site—www.fedworld.gov—with some of the privacy components discussed. These include a home page with a link to the privacy and security statements, a notice about the use and purpose of cookies, and an order form showing a "cookie warning" issued by the browser.

Figure 6: FedWorld Home Page Displaying Links to the Privacy and Security Statements



For each web site visited, we printed the site's home page, privacy statement or disclosure notice, security statement, any other page referring to the site's information practices, and any cookie notices found. Each site was then reexamined by a second individual to identify additional information practice disclosures.

Third-Party Cookies

All sites were also examined for third-party cookie placement. The browsers were set to alert us if a cookie was being placed. If an alert indicated that a web site other than the visited site was attempting to set a cookie, we noted this on a data-collection instrument and printed a copy of the request. A second individual would then recheck the site to ensure accuracy. We considered a third-party to be placing a cookie if we clicked on any link on the site and received a notice that a third-party wished to do so.

Content Analysis

Content analysis consisted of review of all of the information collected. We used six content analysts who worked in teams of two. (One content analyst had also visited sites, but not the same ones he analyzed.) Each team was assigned a certain number of agencies' web sites to review. For each team, one content analyst reviewed half the files, while the other reviewed the other half; they then switched files for review. After both analysts had individually reviewed the complete set of files and filled out a content data-collection instrument for each file, the team met to reconcile any differences in their responses. If the team members could not agree, they discussed their differences with an independent staff member who helped facilitate the reconciliation. Finally, team members completed a new, joint form for each web site. These team answers were considered the final answers for each of the web sites for our reporting purposes. This process was the same as that used by FTC when analyzing commercial web sites.

ENCLOSURE IV ENCLOSURE IV

HOW COOKIES ARE MADE

A cookie is information, not a computer program—a short string of text that is sent from a web server to a web browser when the browser accesses a web page.[16] The information stored in a cookie includes the name of the cookie and its value, its expiration date, and domain name. 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. This information allows the server to recognize returning users, track online purchases, or maintain and serve customized web pages.

When a browser sends the web page request to a server, it includes the name of the Internet domain (such as gao.gov) from which the request is made, an IP (Internet Protocol) address,[17] the type of browser (such as Netscape Communicator or Microsoft Internet Explorer) and the operating system of the client computer, the date and time of the request, and the web pages visited. This information is then stored in the server's log files. A copy of a cookie sent along with this request adds only the information that is contained in the cookie, which was originally sent by the server. Thus, the cookie itself does not provide the server with any additional personal information but makes it easier for the server to track users' browsing habits.

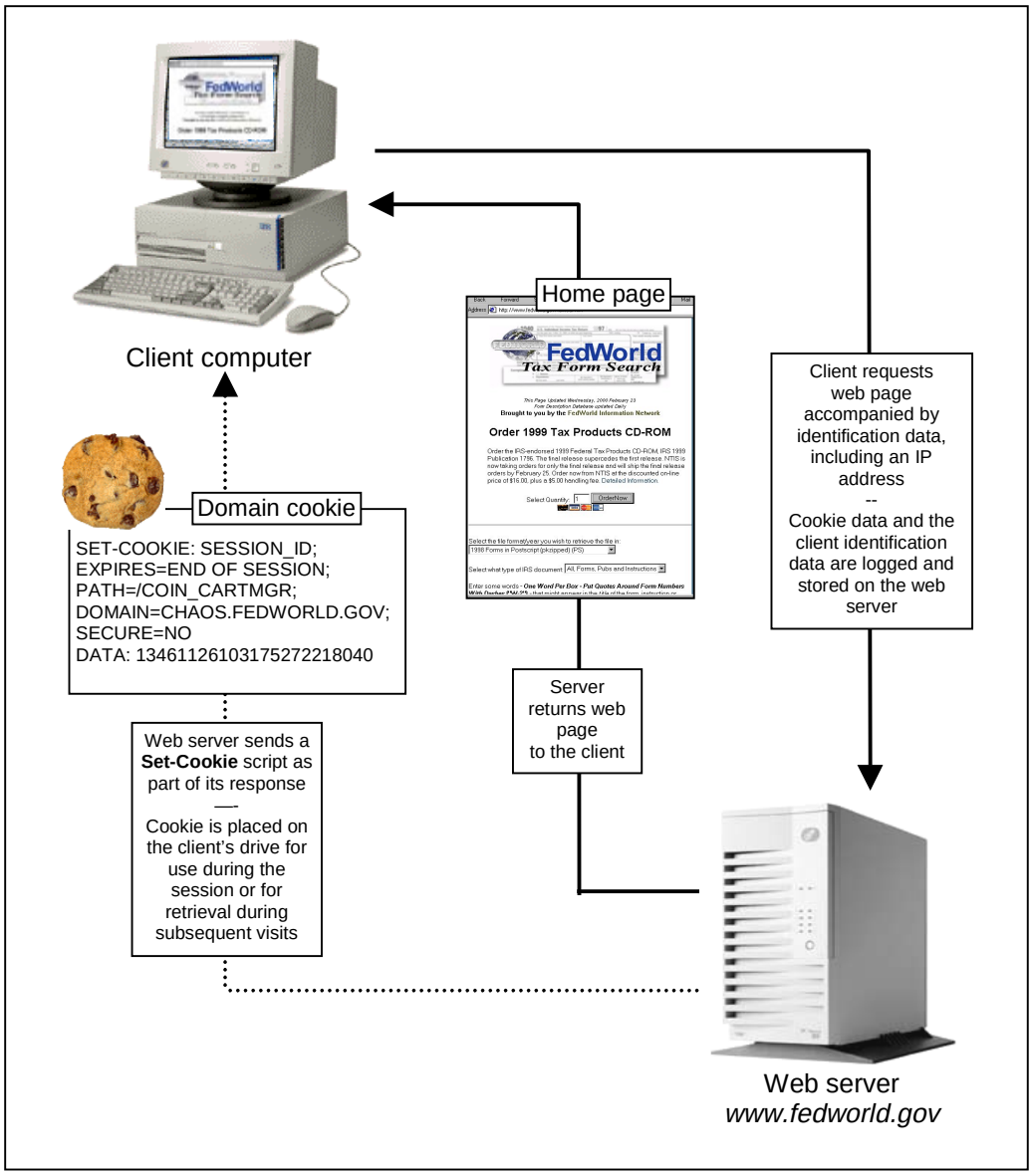
[16]The information in this section draws heavily on the March 12, 1998 Information Bulletin "I-034: Internet Cookies" issued by the Computer Incident Advisory Capability of the Department of Energy.
[17]IP address (Internetwork Protocol address or Internet address) is a unique number assigned by an Internet authority that identifies a computer on the Internet. The number consists of four groups of numbers between 0 and 255, separated by periods (dots). For example, 195.112.56.75 is an IP address.

Different Flavors of Cookies

Cookies come in various flavors—session cookies, persistent cookies, domain cookies, and third-party cookies. Session cookies are short-lived, are used only during the surfing session to facilitate browsing, and expire when the user quits the browser. Persistent cookies specify expiration dates and remain stored on the client's computer until that date, and can be used to track user's browsing behavior by identifying them—or rather their IP addresses—whenever they return to a site. Both the session and persistent cookies are used by Internet shopping sites to keep track of the contents of a shopping cart, but only persistent cookies may be used to create and store customized user profiles and home pages and to track them on multiple web sites within a single domain. Without cookies, electronic commerce activities—including on-line credit card payments and electronic signatures—would be difficult.

Figure 7 shows a simple diagram of a domain cookie being placed by a federal web site. The session cookie is used by the site to process an on-line order requiring an electronic payment.

Figure 7: Domain Cookie



Third-Party Cookies

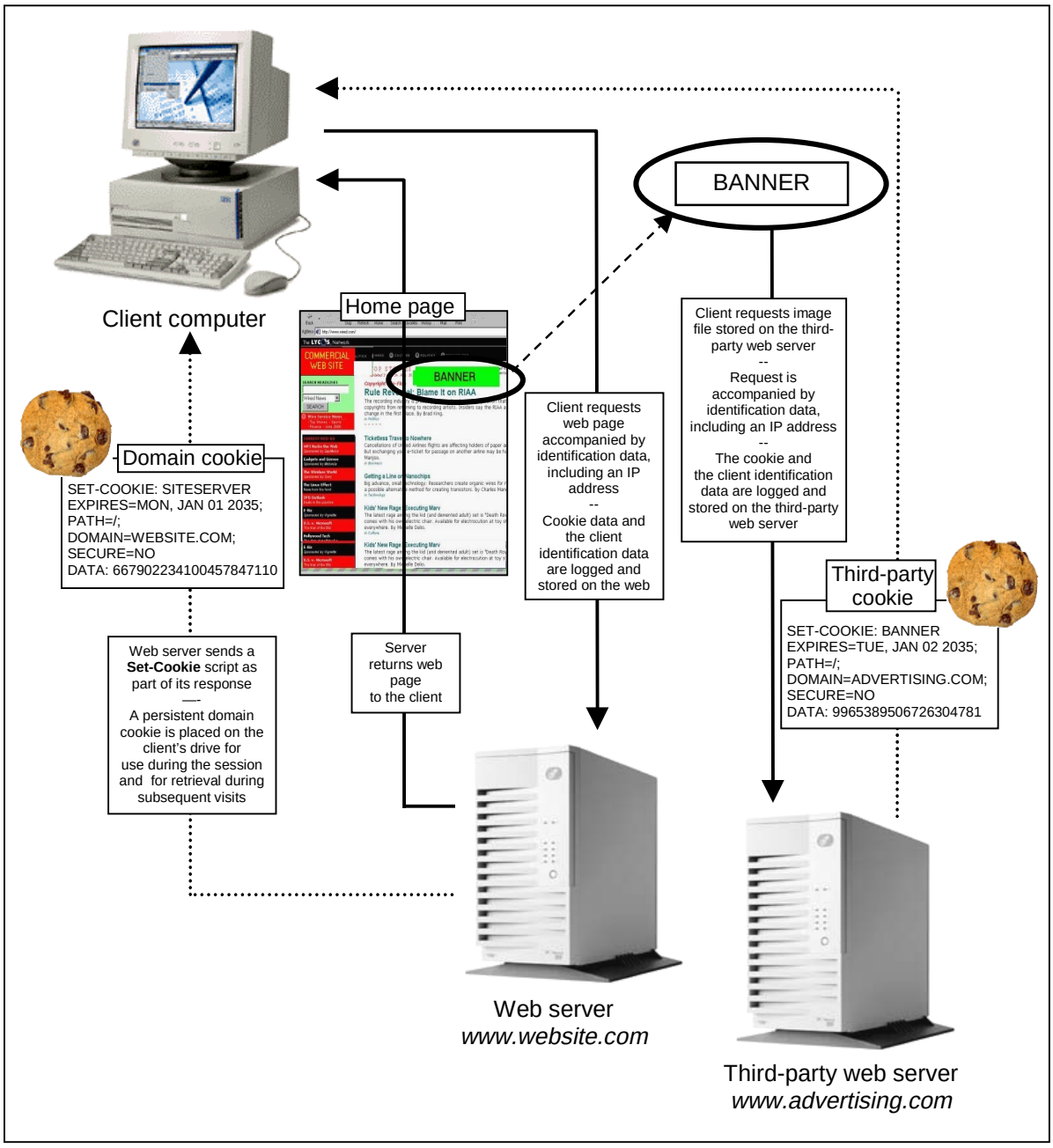
Although domain cookies can be used to see what web pages users have visited and how often they visited them, this information is already in the server's log files. Thus, while cookies do not provide additional identifying information, cookies make it easier for the web servers to track users. However, unlike domain cookies that track users' surfing behavior within a single domain, the third-party cookies allow marketing firms to track user browsing habits on multiple domains with multiple web sites.[18]

In a domain with multiple web sites under contract to a marketing firm, third-party cookies can be used to track user browsing habits on all of the affiliated web sites. The marketing firm contracts with multiple sites to display its marketing, and embeds a tag on their web pages displaying the image of an advertising banner. The image tag does not point to an image on the client's machine but contains the URL (address)[19] of the image file stored on the marketing firm's server. As shown in figure 8, the marketing firm sends a cookie along with the advertisement, and that cookie is sent back to the marketing firm the next time the user views any page containing its advertisement. If the marketing firm contracts with many domains, the firm will be able to track users' browsing habits for long periods of time on many web sites and web pages. This information can be used to infer user interests. However, concern among many is that the information—the IP addresses and "surfing" data collected by the third-party cookies—may be matched with the personal identifying information (name, telephone number, address, credit card number) provided by users to the operators of web sites. Such matching would allow organizations placing third-party cookies to develop detailed personal profiles of web users.

[18]In July 2000, FTC published the second part of its report on this practice known as "online profiling," *Online Profiling: A Report to Congress, Part 2 Recommendations*. The report (1) commended industry leaders who have developed a self-regulatory scheme consistent with fair information principles and (2) recommended that the Congress consider legislation establishing a base level of privacy practices for all consumer-oriented web sites with respect to online profiling.

[19]The URL (uniform resource locator) is a character string specifying the location of an object, typically a web page, on the Internet.

Figure 8: Domain and Third-Party Cookies



(512014)