
Office of Inspector General
Audit Report

**Follow Up on
Privacy Concerns for
Web Visitors**

Department of Transportation

Report Number: FI-2001-019
Date Issued: January 25, 2001



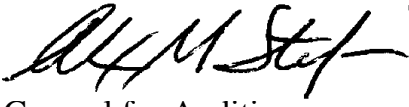


U.S. Department of
Transportation
Office of the Secretary
of Transportation
Office of Inspector General

Memorandum

Subject: **ACTION:** Report on Follow Up on
Privacy Concerns for Web Visitors, DOT
FI-2001-019

Date: January 25, 2001

From: Alexis M. Stefani 
Assistant Inspector General for Auditing

Reply To
Attn Of: JA-20: x61496

To: Heads of Operating Administrations
Director, Bureau of Transportation Statistics
Director, Transportation Administrative Service Center
Chair, Surface Transportation Board
Deputy Chief Information Officer, DOT

In November 2000, the Office of Inspector General (OIG) reported¹ on improper use of cookies² to collect information from the public who visit the Department of Transportation (DOT) web sites. DOT Operating Administrations (OAs) were directed by the Deputy Secretary to improve web privacy protection and to certify 100 percent compliance with the Office of Management and Budget (OMB) and DOT policies.

To reinforce the Deputy Secretary's directive, the OIG agreed to make spot checks after certification of compliance had been filed with the DOT Chief Information Officer (CIO). Our audit objective is to validate the OAs' certification of compliance with OMB and DOT policies concerning the use of cookies.

BACKGROUND

There are two types of cookies—"persistent cookies" and "session cookies." Persistent cookies track information over time and across web sites and remain stored on visitor computers until the specified expiration date. Session cookies are used only during a single browsing session and do not collect information in ways that raise privacy concerns. DOT policy requires the OAs to disclose any use of cookies and to obtain the Secretary's approval for using persistent cookies. As of December 31, 2000, the OAs, except the Federal Aviation Administration (FAA), had certified their compliance with DOT policy. FAA was still in the process of reviewing its 40,000

¹ Report on Privacy Concerns for Web Visitors, Report Number FI-2001-006, November 3, 2000.

² In the Internet world, the term "cookie" represents a mechanism used on web sites to collect information by placing small bits of software on web users' computers.

web pages. None of the OAs had requested the Secretary's approval for using persistent cookies.

On December 21, 2000, Congress passed legislation that requires the OIG to report to Congress by February 19, 2001, on any collection of personally identifiable information on Internet sites. Such information could be collected either on agencies' web sites or through third-party agreements. This report does not address DOT agreements with third parties, if any, pertaining to the collection of personally identifiable information. This issue will be addressed in a separate report to Congress.

SCOPE AND METHODOLOGY

DOT has about 152,000 web pages available for the public's access through its Home Page. From this population, we selected a statistical sample of 797 web pages for testing—98 for FAA and 699 for the remaining OAs (see Exhibit A). We used an optional feature offered by the Microsoft browser to identify the use of cookies. If we found evidence of the use of cookies, we checked for proper approval and disclosure.

The audit was conducted in accordance with Government Auditing Standards prescribed by the Comptroller General of the United States. Follow-up audit work to our November 3, 2000, report was performed in November and December 2000, at DOT and OA Headquarters in Washington, D.C.

RESULTS

DOT Web Pages

Our sample test of 699 web pages (excluding FAA) did not identify any use of persistent cookies³. We identified four session cookies and their usage was disclosed with appropriate privacy statements, as required by DOT policy. Although our sampling revealed no privacy issues concerning the design of DOT web sites, we identified two issues warranting management attention.

- We found incidents that DOT web pages are linked to non-Government web sites that use persistent cookies without any disclosure. Linkage to non-Government sites is created when visitors "click" on web links provided on DOT web sites. Visitors are then notified about leaving DOT sites. At that time, some DOT web sites require visitors to initiate another action, such as clicking on "continue" before the linkage could be completed. Conversely, other DOT web sites automatically establish the linkage within seconds without giving visitors an option to terminate

³ Although we did not identify any use of persistent cookies in our sample, based on probability theory, we are 95 percent confident that there are no more than 449 unauthorized persistent cookies on all DOT websites (excluding FAA).

the connection. This automatic linkage resulted in persistent cookies designed by non-DOT web sites being placed on visitors' machines as a result of their visit to DOT web sites.

For example, 45 of the 96 web pages we sampled in the Federal Transit Administration had automatic linkage. Seven linkages to non-Government web sites resulted in persistent cookies being placed on DOT web visitors' machines (see Exhibit B) without appropriate disclosure. Our sample did not identify such automatic linkages in other OAs; however, there is no assurance that this design is not being used. Proper linkage to non-Government sites should be specified as a requirement in the DOT web configuration checklist, which the departmental CIO Office has agreed to develop.

- In our November 2000 report, we reported that two OAs inadvertently created persistent cookies as a result of improper software configuration on their web sites. During our follow-up review, we found a similar incident on a key home page. This home page was not part of our sample for this report. We had examined it in August 2000 and found no cookies.

In December 2000, the home page went through a major redesign. When OIG visited the revised home page, we found the use of persistent cookies had been activated due to software reconfiguration on the web server. The use of cookies was immediately stopped after we brought it to management's attention. However, this incident demonstrates that protecting web privacy is an ongoing challenge because web sites are revised frequently. The CIO Office's web configuration checklist should cover both new web development and revisions to existing sites.

FAA Web Pages

Our separate test of 98 FAA web pages identified the use of persistent cookies without the Secretary's approval and the use of session cookies without proper disclosure⁴. In our November 3, 2000, report, we recommended, and the departmental CIO concurred, that any use of persistent cookies be disabled until the Secretary's approval had been obtained. This included the use of persistent cookies that the OAs intended to justify for continued use.

FAA should immediately disable the use of persistent cookies detected by OIG and through its own inspection. FAA also should accelerate its inspection of web pages for compliance with DOT policy. We discussed these issues with the FAA CIO who agreed to complete inspecting all FAA web pages by January 31, 2001.

⁴ A memorandum with detailed findings was issued to FAA's CIO on January 3, 2001, for timely correction.

RECOMMENDATIONS

We recommend that the DOT Deputy Chief Information Officer:

1. Incorporate provisions in DOT's web configuration checklist for:
 - a. Building connections to non-Government web sites. DOT web visitors should be given opportunities to terminate the connection after being notified about leaving Government sites.
 - b. Revising existing web sites. Web sites experiencing major revisions should be subject to the same review and approval process as new web development projects.
2. Require the OAs to review their existing web design by January 31, 2001, to ensure that automatic linkage to non-Government web sites is not being used.
3. Work with FAA to ensure persistent cookies detected on FAA web pages are immediately disabled and steady progress is made to ensure FAA's compliance with DOT web privacy policy by January 31, 2001.

MANAGEMENT RESPONSE

A draft of this report was provided to the DOT Deputy Chief Information Officer on January 18, 2001. He agreed with the recommendations, and will take corrective actions by January 31, 2001.

ACTION REQUIRED

In accordance with DOT Order 8000.1C, we would appreciate receiving your written comments within 5 days. If you concur with our findings and recommendations, please state specific actions taken or planned for each recommendation and provide target dates for completion. If you do not concur, please provide your rationale. You may provide alternative courses of action that you believe would resolve the issues presented in this report.

We appreciate the courtesies and cooperation of DOT representatives. If you have questions concerning this report, please call me at (202) 366-1992 or John Meche at (202) 366-1496.

#

DOT Web Pages

Operating Administration	Number of Web Pages and Data Files	Number of Web Pages	Test Sample Size
FAA	59,881	39,755	98
USCG	40,522	33,698	98
FHWA	33,737	21,743	97
BTS	18,123	15,505	97
TASC	9,512	9,816	29
OST	8,245	7,658	29
STB	6,817	6,773	29
FTA	6,879	6,514	96
NHTSA	4,918	4,571	29
RSPA	8,436	1,993	29
FMCSA	1,288	1,220	29
FRA	1,275	1,123	29
MARAD	1,232	1,045	29
OIG	615	368	28
SLSDC	0	133	26
Others	380	32	25
Total	201,860	151,947*	797

*In our November 2000 report, we identified a total of 201,860 web pages and data files that can be accessed from the DOT Home Page. Through further processing, we were able to separate web pages from data files. Only web pages are capable of bearing cookies. The 151,947 web pages represent a snap shot of DOT web sites on November 21, 2000.

Automatic Linkage to Third-Party Web Sites

Number	Organization	Cookie Type
1	Rockwell International	Persistent
2	Major League Baseball	Persistent
3	National Basketball Assoc.	Persistent
4	National Baseball Assoc.	Persistent
5	National Football League	Persistent
6	National Football League	Persistent
7	National Hockey League	Persistent
8	America Online	Session
9	Dept. of Labor	None
10	Washington State DOT	None
11	Commercial Org.	None
12	Federal Highway Administration	None
13	Pierce Transit Washington St.	None
14	Lee County Transit	None
15	Government Printing Office	None
16	Schrock School	None
17	Waco Texas	None
18	Intelligent Transport Sys.Org	None
19	Penn State University	None
20	Tri-met Transit Org.	None
21	Transit Info Organization	None
22	California DOT	None
23	New York City Transit	None
24	Miami Valley RTA	None
25	LA Public Schools	None
26	Bike Map Organization	None
27	Volpe	None
28	Bloomington IN	None
29	RIPTA Company	None
30	Alaska Tourism	None
31	Educational Organization	None
32	Bucknell University	None
33	Small Business Administration	None
34	Vermont Times	None
35	Bay Area Rapid Transit	None
36	Government Printing Office	None
37	Kornet Organization	None
38	Government Printing Office	None
39	Employment and Training Adm.	None
40	Transit Info Organization	None
41	Syracuse U. Bus Schedule	None
42	Government Printing Office	None
43	Council of Fresno, CA	None
44	Glendale Ca Bus Schedule	None
45	Bucknell University	None