Report on Web Privacy

Department of Transportation

Report Number: FI-2001-034
Date Issued: February 26, 2001

Memorandum

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

Subject: **ACTION**: Report on Web Privacy, DOT FI-2001-034

Date: February 26, 2001

Reply To Attn Of: Meche:x61496

From: Alexis M. Stefani
Assistant Inspector General for Auditing

To: Deputy Chief Information Officer, DOT

In December 2000, Congress passed the Fiscal Year 2001 Consolidated Appropriations Act (Public Law 106-554). The Act requires the Office of Inspector General at each Federal agency to report on the agency's collection and review of personally identifiable information on either the agency's Internet sites or through third-party agreements. A third-party agreement allows another Government agency or a non-Government entity to collect personally identifiable information on Internet sites for the agency's use.

Our objective was to determine whether the Department of Transportation (DOT) collects and reviews personally identifiable information about individuals who access DOT or third-party Internet sites.

BACKGROUND

We began reviewing DOT's procedures for protecting the public's privacy on Internet sites in August 2000. We issued two audit reports[1] which focused on whether DOT complied with the Office of Management and Budget (OMB) policy concerning the use of cookies--one of the principal technologies used to collect information from web visitors. We also testified on this subject in September 2000[2].

The term "cookie" has been used in the computer science field for years. In the Internet world, it represents a mechanism used on web sites to collect information by placing small bits of data on web users' computers. There are two types of cookies--"persistent" and "session" cookies. Persistent cookies track information over time and

[1] Report on Privacy Concerns for Web Visitors, Report Number FI-2001-006, November 3, 2000.
Follow Up on Privacy Concerns for Web Visitors, Report Number FI-2001-019, January 25, 2001.

[2] Statement of Kenneth M. Mead Before the Committee on Science, U.S. House of Representatives, Computer Security within DOT, September 27, 2000.

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.

OMB requires Federal agencies, when using persistent cookies, to (1) post clear notices advising visitors of their usage; (2) display privacy statements explaining how the collected information is used; and (3) have a compelling need to gather the data on web sites with the approval by the head of the agency. In DOT, use of persistent cookies requires the Secretary's approval.

SCOPE AND METHODOLOGY

DOT has about 152,000 web pages available for the public's access through its home page, all of which are capable of delivering cookies. We examined home pages on 177 web sites and sampled 1,270 web pages (see Exhibit A) to determine whether the public's privacy was protected when visiting DOT web sites. 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.

For third-party agreements, we surveyed all DOT agencies to determine whether DOT collects and reviews personally identifiable information on non-DOT Internet sites.

The audit was conducted in accordance with Government Auditing Standards prescribed by the Comptroller General of the United States. Audit work was performed from August 2000 through February 2001 at DOT and its Operating Administration Headquarters in Washington, D.C.

RESULTS

DOT Internet Sites

After we first reported unauthorized use of persistent cookies on DOT web sites in our September 2000 testimony, the Deputy Secretary directed DOT agencies to improve web privacy protection and to certify 100 percent compliance with OMB and DOT policy. As of December 31, 2000, all DOT agencies, except the Federal Aviation Administration (FAA), certified they were in compliance. FAA was in the process of reviewing its web pages.

In January 2001, FAA initiated a major effort to examine its web privacy protection and reported eliminating more than 80 unauthorized uses of persistent cookies. On January 31, 2001, FAA certified it was in compliance with the DOT web privacy policy. None of the DOT agencies requested the Secretary's approval to use persistent cookies.

Our audit work in February 2001 identified continued unauthorized use of persistent cookies on FAA web sites. FAA reported that none of these persistent cookies was intentionally designed to collect personally identifiable information from web visitors.

We confirmed that use of unauthorized persistent cookies was associated with either improper software configuration (setup) on web sites or the use of a particular web development tool. Because of the default setting on the web development tool, the use of persistent cookies was unknowingly introduced on web sites. Although not intentional, this inadvertent use of persistent cookies was a privacy violation because the cookies were placed on the visitors' machines as a result of their visit to DOT web sites.

In summary, between August 2000 and February 2001, we identified 22 DOT web pages using unauthorized persistent cookies. The General Accounting Office also identified one in December 2000. Twenty of the 23 were FAA web pages. As of February 20, 2001, the use of persistent cookies on all 23 web pages had been eliminated or the associated web sites were disabled (see Exhibit B).

Through this review process, DOT has learned that protecting web privacy is an ongoing challenge. For example, we examined a key DOT home page in August 2000 and found no cookies. In December 2000, the home page was re-designed. When we visited the revised home page, we found the use of persistent cookies had been activated due to software re-configuration on the web server. The use of cookies was stopped immediately after we brought it to management's attention. However, this incident demonstrates that protecting web privacy is an ongoing challenge because web sites are constantly revised or reconfigured.

As we recommended, the DOT Chief Information Officer developed a "Cookie Use Checklist" requiring all DOT agencies to periodically check their web sites. The checklist should be enhanced to require periodic re-certification for web privacy protection. A mechanism also should be developed to promote information sharing among DOT agencies on inadvertent use of cookies resulting from configuration or web development problems.

Third-party Agreements

We surveyed all DOT agencies to determine whether any DOT internal agency collects and reviews personally identifiable information on non-DOT Internet sites. We found that three DOT contractor web sites were collecting personal data.

E-commerce Contractor. The Bureau of Transportation Statistics (BTS) hires a contractor to distribute its publications. The general public can order BTS publications on-line on the contractor's web site. We were informed by the contractor that it was collecting personally identifiable information on its web site; however, this

information was used only to assist the web visitors' purchasing process. This information was not collected for any other purpose and DOT did not receive the information from the contractor for review. Based on BTS instructions, the contractor stopped this practice in November 2000.

In February 2001, we found a new persistent cookie on this contractor's web site. According to BTS and its contractor, this cookie was inadvertently caused by the same web development tool used on DOT web sites. The use of this persistent cookie was stopped immediately after we brought this to management's attention.

Library Services Contractors. DOT has contracts with two companies that provide subscription services, which allow authorized users to access database information and electronic journals through the companies' web sites. These contractors collect personally identifiable information such as user identification, databases accessed, and web-usage time from visitors. The contractors forward this information to DOT concerning DOT employees' access. DOT is using this information only for billing and usage monitoring purposes.

Based on our review of these contractor web sites, there are no privacy violations because collection of personally identifiable information was either terminated or was limited to DOT employees' on-line access.

RECOMMENDATIONS

We recommend that the DOT Deputy Chief Information Officer:

1. Issue the updated Cookie Use Checklist requiring periodical re-certification from DOT agencies to ensure web privacy protection on DOT web sites.

2. Require DOT agencies to inform the DOT Chief Information Officer when experiencing inadvertent cookies introduced by web configuration or development tools. This information should be shared timely with all DOT agencies.

MANAGEMENT RESPONSE

A draft of this report was provided to the DOT Deputy Chief Information Officer on February 21, 2001. He agreed with the recommendations, and will take corrective actions by March 15, 2001.

ACTION REQUIRED

In accordance with DOT Order 8000.1C, we would appreciate receiving your written comments within 15 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 rational. You may provide alternate 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, please call me at (202) 366-1992 or John Meche at (202) 366-1496.

#