"Who Has Their Hand in the Cookie Jar?"

Preliminary Findings of Federal Agency Web Sites that Use Information-Collecting Devices Without Informing the Public

Federal Agency	Kind of Cookie	Privacy Policy Says . . .
Bureau of Labor Statistics	Persistent[1] & Session Domain	. . . nothing about cookies.
Bureau of Land Management	Session[1] Domain	. . . nothing about cookies.
Central Federal Lands Highway Division	Session Domain	. . . nothing about cookies.
Customs Service	Persistent[1] Third-Party	. . . nothing about third-party cookies.
Department of Energy's Ames Laboratory	Persistent Domain	(No posted privacy policy.)
Federal Aviation Administration	Session Domain	. . . that the agency does not allow the placement of cookies.
Federal Emergency Management Agency	Persistent Third-Party	. . . nothing about third-party cookies.
Forest Service	**Persistent & Session Third-Party**	**. . . nothing about third-party cookies. A private company mines citizens' information from the agency Web site.**
Health Care Financing Administration	Session Domain	. . . nothing about cookies.
National Park Service	Session Domain	. . . nothing about cookies.
Office of National Drug Control Policy	**Session Domain**	**. . . that the agency does not allow the placement of cookies.**
Office of Personnel Management	Session[1] & Persistent Domain	. . . that the agency does not allow the placement of cookies.
U.S. Trade and Development Agency	Persistent Domain	. . . that the agency does not allow the placement of cookies.

Cookie: Code sent to a Web surfer's computer to identify the computer and track the user's surfing habits. All agency Web sites are required to post privacy policies that clearly explain whether and how they use cookies.
Session: Describes a cookie that expires when the Web surfer closes his/her browser at the end of a session.
Persistent: Describes a cookie that lasts a fixed period of time, potentially for years. According to a September 5th OMB guidance, persistent cookies raise serious concerns because they make it "technically easy" for the agency to

learn the complete history of users' Web surfing.
Domain: Describes a cookie that is sent from the Web site that the Web surfer is visiting.
Third Party: Describes a cookie that is sent from a source other than the Web site being visited.

1 These cookies have been removed since the investigation began.

Examples of Administration's Failure to Protect Personal Privacy

Recently, Senator Fred Thompson, Chairman, Committee on Governmental Affairs, documented the Administration's failure to protect personal privacy. Below is a summary of the information developed by Chairman Thompson, including extensive evidence of the Administration's failure to protect taxpayer data, veterans' medical records, citizens' financial records, and sensitive proprietary and confidential business information.

- In March, a routine inventory check of State Department computers revealed that 18 laptop computers were missing. *At least one computer belonged to the State Department's Bureau of Intelligence and Research and is believed to have contained highly classified information. On August 9, 2000, the FBI posted a $25,000 reward for any information leading to its recovery*. [United Press International, "Reward Offered for Information on Missing State Department Computer," August 9, 2000.]

- In June, *the White House confirmed that its Web site for the Office of National Drug Control Policy used cookies to track how visitors used the site*. This activity raised questions from privacy groups and Congress and led to a memo from OMB reiterating the Administration's privacy policy that "privacy policies must be clearly labeled and easily accessed when someone visits a Web site." [Federal Computer Week, "OMB Counters 'Cookies'," June 26, 2000.]

- In July, GAO concluded that the Environmental Protection Agency's computer security controls are so weak that its computer systems are highly vulnerable to tampering, disruption, and misuse from both internal and external sources. Additionally, GAO found that the *EPA could not ensure the protection of sensitive business and financial data maintained on its larger computer systems or supported by its agency-wide network. The information at risk included enforcement-sensitive data, proprietary and confidential business information, and Privacy Act data*. [GAO/AIMD-00-215, "Information Security: Fundamental Weaknesses Place EPA Data and Operations at Risk," July 2000.]

- In 1999, GAO reported that over the last seven years the U.S. Department of Agriculture's Inspector General reported that USDA's National Finance Center, which annually makes over $21 billion in payroll disbursements to about 434, 000 employees, had not ensured that (1) systems security adequately prevented misuse or unauthorized modifications, (2) *access to data was needed or appropriate*, and (3) modifications to software programs were properly authorized and tested. [GAO/T-AIMD-99-146, "The Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection Over Systems and Sensitive Data," April 15, 1999.]

- In September 1998, GAO reported that computer control weaknesses at the Department of Veterans Affairs placed critical operations such as financial management, health care delivery, benefit payments, and life insurance services at risk of misuse and disruption. In addition, *sensitive information contained in the department's systems, including financial transaction data and personal information on veteran medical records and benefit payments, was vulnerable to inadvertent or deliberate misuse, improper disclosure, or destruction–possibly occurring without detection*. [GAO/AIMD-98-175, "VA Information Systems: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure," September 23, 1998.]

- In 1998, GAO conducted a review of 24 of the largest Federal agencies and found serious weaknesses in the government's ability to adequately protect: (1) federal assets from fraud and misuse; (2) *sensitive information from inappropriate disclosure*; and (3) critical operations, including some affecting safety, from disruption. According to the report's conclusions, these weaknesses place critical government operations, such as national defense, tax collection, law enforcement and benefit distribution, at risk. [GAO/AIMD 98-92, "Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk," September 1998.]

- In 1998, GAO's reviews and testing revealed the susceptibility of the State Department's systems to unauthorized access and that unauthorized retrieval of sensitive information from such systems was possible. *Specifically, testers were able to download, delete, and modify data, add new data, shut down servers, and monitor network traffic*. Moreover, this activity went largely undetected, further underscoring the State Department's serious vulnerability to attack. [GAO/AIMD 98-145, "Computer Security: Pervasive, Serious Weaknesses Jeopardize State Department Operations," May 1998.]

- In November 1997, the Social Security Administration Inspector General reported that security weaknesses subjected sensitive information to potential unauthorized access, modification, or disclosure. The Inspector General reported that 29 convictions involving agency employees were obtained during fiscal year 1997, most of which involved creating fictitious identities, fraudulently selling social security cards, misappropriating funds, or abusing access to confidential information. [GAO/T-AIMD-98-312, "Information Security: Strengthened Management Needed to Protect Critical Federal Operations and Assets," September 23, 1998.]

- In 1997 GAO designated information security as a government-wide high-risk area because growing evidence indicated that controls over computerized operations were not effective and there was *compelling information that risks were increasing and personal and national security data was at risk of being compromised*. [GAO/HR-97-1, "High Risk Series: An Overview," February 1997, and GAO/HR-97-9, "High Risk Series: Information Management and Technology," February 1997.]

Examples of Administration's Failure to Protect Personal Privacy

- GAO reported that "weaknesses in IRS computer security controls continue to place IRS's automated systems *and taxpayer data at serious risk to both internal and external attack*." For example, unauthorized employees were given access to sensitive computer areas while employees whose jobs did not require it were given the ability to change, alter, or delete taxpayer data. Additionally, *the GAO reported that the IRS could not account for a total of 397 missing computer tapes (some of which contained sensitive taxpayer data or privacy information) and found that tapes and disks containing taxpayer data were not erased prior to reuse (thus potentially allowing unauthorized access to sensitive data)*. [GAO/AIMD 97-7, "IRS Systems: Tax Processing Operations and Data Still at Risk Due to Serious Weaknesses," April 1997.]

- In 1996 GAO reported that *audit reports and self assessments completed by Federal agencies showed that weak information security put billions of dollars of Federal assets at risk of theft, misuse or loss, and threatened the vast amount of sensitive data, including personal data on individuals, with unauthorized disclosure*. [GAO/AIMD-96-110, "Information Security: Opportunities for Improved OMB Oversight of Agency Practices," September 24, 1996.]

- According to a report issued by the GAO in 1996, unauthorized individuals are increasingly attacking and gaining access to highly sensitive unclassified information on the Department of Defense's systems. In fact, the report noted that these *attacks can range from being multimillion dollar nuisances to being a serious threat to national security*. [GAO/AIMD-96-84, "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks," May 22, 1996.]

- In 1995, allegations were made that the Idaho National Engineering Laboratory sold surplus computer equipment that contained sensitive data to an Idaho businessman. GAO investigated the allegations and *concluded that some of the computers sold may have contained sensitive data, but did not determine how many*. GAO added that, like all Federal agencies, the Department of Energy is required to establish computer security safeguards, yet it had not. [GAO/AIMD 95-11, "Department of Energy Procedures Lacking to Protect Computerized Data," June 1995.]