GAO
Accountability * Integrity * Reliability

GAO Assignments on Privacy & Their Relationship to CSSPAB's Proposed Recommendations

Briefing for the

Computer System Security & Privacy Advisory Board
(CSSPAB)

National Institute of Standards and Technology
Department of Commerce

Scheduled for September 17, 2002

by Alan Stapleton

GAO
Accountability * Integrity * Reliability

Introduction

GAO has four privacy projects under way that appear related to recommendations in this board's May 2002 exposure draft ("Findings and Recommendations on Government Privacy Policy Setting and Management"):

- A comprehensive survey of 25 agencies' privacy policies and practices.
- An executive guide on promising methods from the public and private sector that agencies can use to better protect the privacy of individuals.
- An evaluation of SSA's policies for disclosing personal information to law enforcement agencies compared to other agencies.
- An update of GAO's September 2000 Report "Internet Privacy: Agencies' Efforts to Implement OMB's Privacy Policy" (GGD-00-191).
  - As part of this update, we developed a standard format (template) for agencies to summarize their Web site privacy policies. I would like your comments on the template at today's meeting.

I will discuss the scope and objectives of each assignment and its relationship to your recommendations.

GAO
Accountability * Integrity * Reliability

(1) Survey of Agencies' Privacy Act Practices

The GAO survey of agencies' Privacy Act practices is related to the CSSPAB draft recommendation to:

- "Document and strengthen privacy management practices across the federal government by identifying and categorizing all privacy officials ... identifying grade and organizational level,location within the agency hierarchy (I.e., reporting chain, assigned authorities and responsibilities, staff size and composition) ....to develop a complete picture and better understanding of the Federal privacy management infrastructure and (2) Publish a one-time report, which examines the differences from agency to agency.....".

GAO
Accountability * Integrity * Reliability

(1) Survey of Agencies' Privacy Act Practices

Objectives: Senator Lieberman and Cong. Horn asked that we answer four questions:

- What is the level of agency compliance with the Privacy Act and related Office of Management and Budget (OMB) guidance?
- To what extent do agency officials believe OMB's guidance and oversight of the act is adequately meeting their needs?
- What changes, if any, do agency officials believe are needed for them to better implement the Privacy Act?
- To what extent do agencies maintain personal information that is *not* subject to the Privacy Act?

GAO
Accountability * Integrity * Reliability

(1) Survey of Agencies' Privacy Act Practices

Methodology: We sent detailed surveys containing questions about these four issues to 25 departments and agencies:

- Departments: Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Housing and Urban Development, Interior, Justice, Labor, State, Transportation, Treasury, Veterans Affairs.
- Agencies: Equal Employment Opportunity Commission (EEOC), Federal Emergency Management Agency (FEMA), Office of Personnel Management (OPM), National Science Foundation (NSF), Office of Government Ethics (OGE), Small Business Administration (SBA), Social Security Administration (SSA), Pension Benefit Guaranty Corporation (PBGC), Federal Trade Commission (FTC), Office of Special Counsel (OSC), Securities and Exchange Commission (SEC).

We selected these agencies to provide a cross section of large, medium, and small agencies that were likely to have different missions and organizational structures and, perhaps, different approaches to implementing the Privacy Act.

GAO
Accountability * Integrity * Reliability

(1) Survey of Agencies' Privacy Act Practices

Methodology (cont'd): We asked these agencies to complete a total of 388 surveys in three separate mailings:

- The first mailing consisted of 25 surveys (one per agency) that asked about agencywide Privacy Act practices and procedures (e.g., how many systems of records exist?). The survey also contained 19 questions about compliance with specific Privacy Act provisions, OMB guidance, and other related laws.
- The second mailing consisted of 204 surveys—one for each of the 185 systems of records that we randomly selected from the population of about 3,600 at these agencies and 19 systems of records we judgmentally selected because they were large important systems. This survey included 25 questions about each system of records' compliance with specific Privacy Act policies and procedures or related OMB guidance.

GAO
Accountability * Integrity * Reliability

(1) Survey of Agencies' Privacy Act Practices

Methodology (cont'd):

- The third mailing, which asked about personal information not subject to the Privacy Act, consisted of 159 surveys—one for each of 150 information systems that we randomly selected from the agencies' budget Exhibits 53 required by OMB Circular A-11 for fiscal year 2002 and 9 that we judgmentally selected based on discussions with officials from agencies that were not required to prepare Exhibit 53.
- Our plan is to brief the Congressional requesters on the survey results at the end of September and then issue a detailed report early next year with conclusions and recommendations.

GAO
Accountability * Integrity * Reliability

(1) Survey of Agencies' Privacy Act Practices

Methodology (cont'd): Among our 41 compliance questions were the following:

- Has your agency issued a Federal Register notice for this systems of records? Did your agency review this notice to ensure that it was accurate?
- For this system of records, would your agency be able to account for all disclosures of individuals' records?
- Has your agency promulgated a final rule under the Administrative Procedures Act that explains why your agency considers exemptions to the act necessary?
- Was this computer matching agreement approved by the Data Integrity Board?
- Since October 1, 2000, did any person, without authorization, read, alter, disclose, or destroy any personal information in this system?
- Since October 1, 1998, has any court ruled that your agency violated any provision of the Privacy Act?

GAO
Accountability * Integrity * Reliability

(1) Survey of Agencies' Privacy Act Practices

Verify Accuracy of Survey Responses: To help ensure the accuracy of answers related to compliance with the Privacy Act or OMB guidance, we randomly selected agencies' responses and asked officials to provide documentation or additional narrative explanations to support their answers.

In addition, when agencies stated in their responses that they had issued certain public documents required under the act (e.g., a regulation), we located and reviewed the documents to be certain that they had been issued.

Since we did not ask questions on the surveys about every provision in the act and we did not perform detailed audit work at these 25 agencies, we do not know whether the actual levels of compliance are different from those that agencies reported.

GAO
Accountability * Integrity * Reliability

(1) Survey of Agencies' Privacy Act Practices

Other survey questions directly address the board's desire for more information on agencies' privacy infrastructure. Examples include:

- Would you consider the organizational structure for implementing the Privacy Act in your agency to be centralized or decentralized (definitions provided)?
- For your entire agency, who has day-to-day responsibility for implementing the Privacy Act? Is this person considered your agency's Privacy Act officer?
- From the head of the agency, how many organizational levels removed is this person?
- In your agency's organization, what is the location of this person? To whom does this person report?
- For fiscal year 2002, about how many FTE staff years will your entire agency spend on implementation of the Privacy Act?

GAO
Accountability * Integrity * Reliability

(1) Survey of Agencies' Privacy Act Practices

Based on responses to other questions in the surveys, we will estimate what percent of the population of 3,600 systems of records were:

- Exclusively electronic records, a combination of manual and electronic, or exclusively manual.
- Operated by the agency or a contractor.
- Exempt from one or more provisions of the Privacy Act.
- Involved in one or more computer matching programs during 2001.
- Allowing the subject individuals to access their personal information via the Web.

In addition, we will identify the number of records that agencies retrieved from systems of records during fiscal year 2001 and the types of personal information most frequently used to retrieve records were (e.g., name, social security number).

Any questions before moving to the next assignment?

11

GAO
Accountability * Integrity * Reliability

(2) Executive Guide: Promising Methods for Agencies to Protect the Privacy of Individuals

Our second assignment -- to develop an executive guide on promising methods for protecting privacy -- is related to the following draft board recommendation:

- "Implement an on-going mechanism to keep abreast of and evaluate emerging private sector policies, technologies, risk management models, and operational systems and practices to evaluate their value to and impact on the government, and to employ them, as appropriate."

If the guide turns out as we hope, it will provide this proposed mechanism with a discussion of emerging private and public sector technologies and models for protecting privacy.

12

(2) Executive Guide: Promising Methods for Agencies to Protect the Privacy of Individuals

This executive guide will identify promising methods from private and public organizations to protect the privacy of personal information that may have application in federal agencies.

- Recognizing the need for more effective homeland security, a broad range of agencies are or will be collecting new kinds of data (e.g., biometrics) and sharing it more often. As a result, new privacy issues are emerging, and new strategies may be needed for privacy protection and data stewardship.
- Key questions: (1) What are examples of emerging data-privacy issues in the new homeland-security environment? (2) For each example, what are actual or potential strategies to protect privacy or assure adequate data stewardship?
- The guide will be organized around the eight OECD fair information practices (FIPs) that underlie the Privacy Act and form the basis of many privacy laws in the United States and around the world.

13

(2) Executive Guide: Promising Methods for Agencies to Protect the Privacy of Individuals

Among the potential private sector models that we are evaluating is the **ISTPA privacy framework** that board members were briefed on in Chicago at your September 2001 meeting. The ISTPA describes the framework as "a template for designing privacy management systems and as an analytic tool for assessing privacy solutions."

It consists of seven services and three capabilities. As you know, a CSSPAB member—John Sabo—is one of the leaders on this effort. Since we are just beginning to examine this framework, I would prefer you direct your questions on it to John.

There are many other promising methods that we are just beginning to explore that I cannot discuss now. We hope to issue the guide in the summer of 2003.

Any questions about this guide before moving to the next assignment?

14

(3) Evaluation of SSA's Policies for Disclosing Information to Law Enforcement Agencies

This third assignment is relevant to the CSSPAB recommendation to:

- "Create mechanisms to ensure that those government officials responsible for the protection of private information understand and can accommodate, to the extent permitted by statute and regulation, the needs for data sharing and data matching enforcement agencies seeking to enhance homeland security."

The Chairs of two subcommittees in the House (Judiciary and Ways and Means) have asked us to:

- compare SSA's policy for disclosing information to law enforcement agencies with the Privacy Act requirements and
- compare SSA's disclosure policy to law enforcement agencies with those of other large departments and agencies.

This work is just beginning, and we do not know when the work will be completed.

Any questions about this new assignment before moving to the next one?

(4) Update of GAO's September 2000 Report on "Internet Privacy" (GGD-00-191)

The fourth and final GAO assignment appears to update our September 2000 report on Internet privacy appears related to the board's draft recommendation to:

- "Perform an examination of national systems of records and databases... This effort should include: .....b. addressing notice, choice and consent issues in the light of e-Government initiatives ... in part to ensure that **consistent policies** [emphasis added] are presented to the public on privacy choices across agencies."

(4) Update of GAO's September 2000 Report on "Internet Privacy" (GGD-00-191)

Our September 2000 report found that most agencies' principal Web sites had privacy policies that were clearly labeled and easily accessed. However, we also found that of 31 high impact agencies, most did not post a privacy policy on all Web pages where personal information was collected.

We are updating two of the objectives in our September 2000 report. Both objectives relate to OMB's June 1999 memorandum that agencies have:

- **clear** and **concise** privacy policies posted on their principal Web sites and pages where substantial personal information is collected, and
- privacy policies that inform visitors what information an agency collects, why it is collected, and how it will be used.

We will determine how 24 major departments and agencies have implemented these OMB requirements. Our original report examined Web sites at 70 agencies.

The final report will not be available until early next year. However, we have developed a draft paper describing our preliminary results on the first objective regarding OMB's "clear and concise" standard.

(4) Update of GAO's September 2000 Report on "Internet Privacy" (GGD-00-191)

Methodology: *(Refer them to handout with draft template)*

- To determine whether agency privacy policies were clear and concise as OMB requires, we first performed a content analysis of the privacy policies at the 24 agencies This entailed carefully reading each of the policies and breaking them down into distinct elements. When we found that more than one Web site used different words to describe the same basic element of privacy, we combined them into one standard privacy statement.

Through this process, we summarized dozens of pages of different text into over 40 such standard elements. We did not use focus groups to evaluate how effectively the wording of the standard elements communicated our intended meaning.

GAO
Accountability * Integrity * Reliability

(4) Update of GAO's September 2000 Report on "Internet Privacy" (GGD-00-191)

Findings: More than 3 years after OMB required agencies' privacy policies to be clear and concise, we found them to be somewhat ambiguous and longer than necessary .

Although OMB's memorandum provided agencies with sample language for use in developing their policies, not all agencies used the language; many used different words to describe the same policy elements.

Agencies also used different formats for presenting the same information. For example, Web sites at the Department of Defense, Veterans Affairs, and the Social Security Administration placed important elements of their privacy policies behind links. Some links were easy to miss because they were located on the margins of the page or were identified only by underlined text rather than italics or a different color that would make them more prominent to Web site visitors.

GAO
Accountability * Integrity * Reliability

(4) Update of GAO's September 2000 Report on "Internet Privacy" (GGD-00-191)

Findings (cont'd):

This diversity in privacy policies, formats, and language makes it necessary for the public to carefully read all parts of the often long and complicated privacy policies at each agency they visit. This may require more effort than some visitors believe is warranted. If so, they may decide not to continue their visit or not to provide their personal information.

Building visitors' confidence and trust may be critical to agencies' success in various e-government initiatives, where users must submit personal information to complete the business transactions involved. Those who have doubts about how their personal information may be used may not choose to participate in e-government initiatives.

Potential Recommendation: To make the presentation of the various complex privacy policies at agency Web sites simpler and more "user friendly," we are considering a recommendation that the Director, OMB, encourage agencies to use a consistent privacy notice format or template to describe the major elements of the agency's policy and relevant OMB guidance.

GAO
Accountability * Integrity * Reliability

(4) Update of GAO's September 2000 Report on "Internet Privacy" (GGD-00-191)

If you would look at the template on page 4 of the handout, only those policies that appeared most frequently in agency policies or that were in OMB guidance are on the template.

The last line on the template would provide a link to a Web page containing supplementary information on all the agency's exceptions, any other details of its privacy policies not adequately reflected on the template, and methods to contact the agency (see example). In this way, agencies could layer the short notice that is easy to read and comprehend on top of the agency's detailed policies, if necessary.

The standard notice format that we propose is considerably shorter and simpler than most privacy statements now in use, and thus it should better communicate key policies. Users would obtain definitions of important terms (e.g., *personal information*) on the notice by clicking on the particular term.

21

GAO
Accountability * Integrity * Reliability

(4) Update of GAO's September 2000 Report on "Internet Privacy" (GGD-00-191)

Under the proposed approach, each agency would identify those standard policies on the template that apply to its site. In addition to having a link to the template from agencies' principal home pages, there could also be a link to it from all pages where substantial personal information is collected.

We believe this will help to avoid frustrating Web site visitors, who must now read complex notices in a variety of formats, which may suggest that an agency is not being as transparent as it could.

22

GAO
Accountability * Integrity * Reliability

(4) Update of GAO's September 2000 Report on "Internet Privacy" (GGD-00-191)

To make it easy for Web visitors to quickly "scan" different agencies' policies, the template is organized so that the privacy protections can be seen at a glance (see example). An "exceptions" column would be provided that highlights those aspects of the agency's policy that are not providing the maximum privacy protections. This allows Web visitors to quickly scan this column only and then decide whether to terminate their visit, to continue the visit, or perhaps to provide personal information if requested.

Like the "Nutrition Facts" labels on food, the elements on the notice would be exactly the same across all agencies, so that Web visitors could quickly become familiar with those policies of greatest concern to them and be able to quickly check those policies at any agency they visit.

GAO
Accountability * Integrity * Reliability

(4) Update of GAO's September 2000 Report on "Internet Privacy" (GGD-00-191)

The wording of the policy elements shown on the template are for illustration purposes only; OMB should consult with the agencies or the CIO Council to develop specific wording that better meets their needs.

Agencies should also perform research using focus groups to determine (1) how effectively the draft template they develop communicates the agencies' intended meanings and (2) whether it is written from the consumers' perspective (rather than the agency's perspective).

GAO
Accountability * Integrity * Reliability

(4) Update of GAO's September 2000 Report on "Internet Privacy" (GGD-00-191)

Private Sector Template: The proposed template for agencies is also consistent with a private sector initiative to develop a short standard privacy notice for consumers use who visit company Web sites. A dozen or so companies are working on this project.

The project is being led by the Center for Information Policy Leadership at Hunton & Williams [1]. They have developed a copyrighted template that is described as covering consumers' most important concerns using standard terminology.

They used focus groups to (1) determine how many privacy elements the public can process without difficulty and (2) what suggested words and phrases they prefer to see in privacy policies.

That sums up our privacy projects and their relationship to this board's draft recommendations. Are there questions on any of these projects? I am particularly interested in your comments on the draft privacy template.

[1] Center for Information Policy Leadership at Hunton & Williams, "The Short Privacy Notices Project," April 16, 2002.