May 2008

PRIVACY

Alternatives Exist for Enhancing Protection of Personally Identifiable Information

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-08-536, a report to congressional requesters

Why GAO Did This Study

The centerpiece of the federal government's legal framework for privacy protection, the Privacy Act of 1974, provides safeguards for information maintained by federal agencies. In addition, the E-Government Act of 2002 requires federal agencies to conduct privacy impact assessments for systems or collections containing personal information.

GAO was asked to determine whether laws and guidance consistently cover the federal government's collection and use of personal information and incorporate key privacy principles. GAO was also asked, in doing so, to identify options for addressing these issues.

To achieve these objectives, GAO analyzed the laws and related guidance, obtained an operational perspective from federal agencies, and consulted an expert panel convened by the National Academy of Sciences.

What GAO Recommends

To address the issues identified by GAO, Congress should consider revising privacy laws in accordance with the alternatives outlined in the report. While OMB could address some of these issues in its guidance to federal agencies, Congress is ultimately responsible for balancing the needs of government and individual privacy rights. OMB commented that the Congress should consider these alternatives in the broader context of all privacy and related statutes.

To view the full product, including the scope and methodology, click on GAO-08-536.
For more information, contact Linda Koontz at (202) 512-6240 or koontzl@gao.gov.

What GAO Found

Increasingly sophisticated ways of obtaining and using personally identifiable information have raised concerns about the adequacy of the legal framework for privacy protection. Although the Privacy Act, the E-Government Act, and related guidance from the Office of Management and Budget set minimum privacy requirements for agencies, they may not consistently protect personally identifiable information in all circumstances of its collection and use throughout the federal government and may not fully adhere to key privacy principles. Based on discussions with privacy experts, agency officials, and analysis of laws and related guidance, GAO identified issues in three major areas:

Applying privacy protections consistently to all federal collection and use of personal information. The Privacy Act's definition of a "system of records" (any grouping of records containing personal information retrieved by individual identifier), which sets the scope of the act's protections, does not always apply whenever personal information is obtained and processed by federal agencies. One alternative to address this concern would be revising the system-of-records definition to cover all personally identifiable information collected, used, and maintained systematically by the federal government.

Ensuring that collection and use of personally identifiable information is limited to a stated purpose. According to generally accepted privacy principles of purpose specification, collection limitation, and use limitation, the collection of personal information should be limited, and its use should be limited to a specified purpose. Yet, current laws and guidance impose only the modest requirements in these areas. While, in the post-9/11 environment, the federal government needs better analysis and sharing of certain personal information, there is general agreement that this need must be balanced with individual privacy rights. Alternatives to address this area of concern include requiring agencies to justify the collection and use of key elements of personally identifiable information and to establish agreements before sharing such information with other agencies.

Establishing effective mechanisms for informing the public about privacy protections. Another key privacy principle, the principle of openness, suggests that the public should be informed about privacy policies and practices. Yet, Privacy Act notices may not effectively inform the public about government uses of personal information. For example, system-of-records notices published in the *Federal Register* (the government's official vehicle for issuing public notices) may be difficult for the general public to fully understand. Layered notices, which provide only the most important summary facts up front, have been used as a solution in the private sector. In addition, publishing such notices at a central location on the Web would help make them more accessible.